

О.М. ЛЕПЕШКИН, О.А. ОСТРОУМОВ, Н.В. МИХАЙЛИЧЕНКО,
А.С. ПЕРМЯКОВ

**МЕТОДИКА ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ
УСТОЙЧИВОСТИ СИСТЕМЫ СВЯЗИ ЗА СЧЕТ ВЫЯВЛЕНИЯ
КОНФЛИКТОВ**

Лепешкин О.М., Остроумов О.А., Михайличенко Н.В., Пермяков А.С. Методика обеспечения функциональной устойчивости системы связи за счет выявления конфликтов.

Аннотация. Введение: Современные сложные технические системы часто бывают критически важными. Критичность обусловлена последствиями нарушения функционирования таких систем, не выполнением ими требуемого перечня функций и задач. Процесс контроля и управления такими системами осуществляется с использованием систем и сетей связи, которые становятся для них критичными. Возникает потребность в обеспечении устойчивого функционирования, как самих сложных технических систем, так и их систем управления, контроля, систем и сетей связи. В работе предложена методика обеспечения функциональной устойчивости системы связи, основой которой является процесс выявления и устранения в ней конфликтов, обусловленных отличием профиля функционирования и профиля процесса функционирования системы. Предложенная модель процесса функционирования системы связи позволяет на основе анализа интенсивностей воздействия дестабилизирующих факторов на систему, выявления конфликтов и их устранения, определить вероятность обеспечения функциональной устойчивости системы. Цель исследования: разработка методики обеспечения функциональной устойчивости системы связи в условиях воздействия дестабилизирующих факторов и возникновения конфликтов, а также модели процесса функционирования системы связи, позволяющей определять вероятность нахождения системы в функционально устойчивом состоянии. Методы теории графов и теории матриц, теории Марковских процессов. Результаты: предложена модель процесса функционирования системы связи в условиях воздействия дестабилизирующих факторов, позволяющая определять вероятность нарушения функционирования системы, разработана методика обеспечения функциональной устойчивости системы связи. Практическая значимость: результаты исследования могут быть использованы при проектировании и построении сложных технических систем, а также в системах поддержки принятия решений, контроля, связи и управления.

Ключевые слова: функциональная устойчивость, критичность, система связи, система управления, сложная техническая система, профиль функционирования системы, функции, задачи, регламент.

1. Введение. Современные системы управления имеют в своем составе системы или сети связи. Значение связи в условиях повсеместной цифровизации и использования информационных технологий значительно возрастает. Системы связи (СС) приобретают важное критическое значение для систем управления (СУ), при этом критичность проявляется в последствиях нарушений функционирования систем, в их неспособности выполнять определенные требуемые задачи и функции. Усложнение системы, увеличение ее возможностей, большая

динамика изменения состояний системы и ее элементов определяют потребность в информации о ее состоянии, а также происходящих в ней процессах. Информация о состоянии СС позволит СУ своевременно влиять на нее для обеспечения ее устойчивого функционирования.

В процессе функционирования на систему, которая выполняет определенный набор функций и задач, воздействуют различные дестабилизирующие факторы (ДФ) [1, 2]. Под ДФ будет пониматься любое воздействие на СС и ее элементы, результатом которого является нарушение ее функционирования.

Под функциональной устойчивостью (ФУ) СС понимается ее способность обеспечивать выполнение функций и задач в условиях воздействия на нее различных ДФ [3, 4].

В работе при оценке ФУ не учитывается осведомленность злоумышленника, уровень его подготовки, квалификация и техническое оснащение, а также характер воздействия и факторы, влияющие на систему [5, 6]. Учитывается только воздействие на СС, результатом которого является нарушение устойчивого функционирования СС и ее элементов, т.е. невыполнение системой функций и задач, профиля функционирования системы [7].

Традиционно устойчивость системы связи рассматривается через надежность [8 – 12], живучесть [13, 14], помехоустойчивость [15, 16] и киберустойчивость [17 – 22], при этом в качестве характеристики устойчивости, как правило, выступает только один параметр. Реже устойчивость рассматривается как свертка показателей перечисленных характеристик. Кроме этого, ряд работ посвящен общесистемным вопросам обеспечения устойчивости сложных технических систем [23 – 26]. Оценка показателей устойчивости осуществляется на основании анализа статистики функционирования СС до момента оценки, что в условиях большой динамики изменения обстановки, а также потребности в получении информации о системе в режиме реального времени, не всегда приемлемо.

В иностранных источниках термины функциональная устойчивость, функциональная надежность и функциональная живучесть используются наравне. Вклад в развитие теории функциональной устойчивости внесли Додонов А.Г., Тарасов А.А., Бородакий Ю.В. [4, 27], Богатырев В.А., Богатырев А.В. [28 – 29], Турута Е.Н. [30 – 31], Кривошея Д.О., Васильев С.В., Демчук В.А., Двилянский А.А., Машков О.А. [32], Королев А.Н. [33], Фирсов С.Н., Климов С.М., Одоевский С.М. и др. В работах этих авторов под функциональной устойчивостью, как правило, понимается функциональная надежность систем и объектов, обеспечение которой

связано только со структурной реконфигурацией системы, объекта. Отличительной особенностью разработанной авторами методики, является предложение на осуществление синтеза не только структуры системы, но и ее функциональной характеристики, определяемой целевым предназначением системы. Кроме того, авторами предложен новый подход формализации системы на основе профиля функционирования системы, а также процесса ее функционирования на основе профиля процесса функционирования системы. В рамках методики разработана новая модель процесса функционирования СС, позволяющая определить вероятность нарушения устойчивого функционирования системы в зависимости от интенсивности воздействия ДФ, интенсивность синтеза системы, влияющего на время ее устойчивого функционирования.

Разработанная методика обеспечения функциональной устойчивости СС в условиях воздействия на нее и ее элементы дестабилизирующих факторов предназначена для должностных лиц, занимающихся планированием связи, а также лиц, которые принимают решение в этой системе. Время, необходимое для синтеза системы, определяет интервал проверки готовности к выполнению текущей задачи, функции.

Синтез СС будет представлять собой функциональный синтез, заключающийся в перераспределении ресурсов для выполнения задач и задач для выполнения функций, а также структурный синтез системы, включающий реконфигурацию физической основы СС.

Цель работы заключается в разработке методики обеспечения ФУ СС, позволяющей в условиях воздействия ДФ и изменения состояний системы, обстановки, выявлять конфликты в ней, обусловленные отличием профиля процесса функционирования системы от профиля функционирования системы в любой момент времени. На основании полученных данных принимать меры для синтеза, как структуры системы, так и ее функциональной характеристики.

Научная новизна полученных результатов заключается в разработке новой методики обеспечения ФУ СС, использующей профиль функционирования системы для выявления конфликтов, обусловленных воздействием на систему различных ДФ. Кроме этого, получена новая модель процесса функционирования СС на основе использовании математического аппарата теории Марковских процессов, которая позволяет оценивать время и вероятность сохранения требуемой ФУ СС.

3. Постановка задачи на исследование. Своевременное обнаружение конфликта в системе связи и правильное реагирование на

него до момента окончания выполнения задачи, функции путем синтеза системы позволит выполнить задачу, функцию и обеспечить ФУ СС, независимо от характера воздействия ДФ.

Оптимизационная задача заключается в поиске такого решения выявления конфликта, при устранении которого требуется задействование минимального ресурса системы, использование которого позволит обеспечить достижение целевого предназначения системы и обеспечить ее ФУ.

Целевую функцию можно представить следующим выражением:

$$\langle W(\vec{E}, j), F \rangle \rightarrow \min \Delta E \mid k_{\text{ФУ}} \leq k_{\text{ФУ треб}}, j \in N, \quad (1)$$

где $W(\vec{E}, j)$ – упорядоченное множество векторов ресурсов СС, обеспечивающих ее функционирование и выполнение целевого предназначения; $j \in N$ – количество элементов СС, характеризующих структуру системы связи; F – интенсивность вариации элементов СС, позволяющих предоставлять системе связи требуемый ресурс; $k_{\text{ФУ}}$ – коэффициент ФУ СС; $k_{\text{ФУ треб}}$ – требуемый коэффициент ФУ СС.

Выходные результаты методики обеспечения ФУ СС в условиях воздействия ДФ и наличия конфликта в системе: $\langle W(\vec{E}, j), F \rangle$.

Перейдем к описанию исходных данных.

Исходные данные методики:

Данные, характеризующие структуру СС: количество элементов в системе $i = \overline{1, N_y}$, где N_y – общее количество элементов в системе, количество связей, соединяющих элементы СС, $k = \overline{1, L}$, где L – общее количество связей в системе, количество технических средств, находящихся на элементах СС и позволяющих формировать связи, при этом направления связи между элементами задаются парами $\langle i, m \rangle \in L$, $i \in N_y$, $m \in N_y$, $j = \overline{1, N_c}$, где N_c – общее количество технических средств связи на элементах СС и $l(j)$ – количество режимов функционирования каждого j -го средства связи, $\lambda_G(i, \lambda_i)$ – множество, характеризующее нагрузку в виде интенсивностей потока сообщений λ_i от i -го УС.

Данные, характеризующие функциональную составляющую СС: множество целей СС $A = \{A_1, A_2, \dots, A_a\}$, множество требований, предъявляемых к СС $T = \{T_1, T_2, \dots, T_n\}$, множество функций, выполняемых СС $F = \{F_1, F_2, \dots, F_c\}$, множество задач, решаемых СС

$Z = \{Z_1, Z_2, \dots, Z_d\}$ и множество ресурсов СС $E = \{E_1, E_2, \dots, E_m\}$, обеспечивающих ее функционирование.

Данные, характеризующие потребности СУ: множество целей СС $A = \{A_1, A_2, \dots, A_d\}$, которые ей необходимо достичь в интересах СУ, множество требований, предъявляемых к системе связи со стороны СУ $T = \{T_1, T_2, \dots, T_n\}$, множество функций, выполняемых системой $F = \{F_1, F_2, \dots, F_c\}$, которые ей необходимо выполнить в интересах СУ, множество задач, решаемых системой связи в интересах СУ $Z = \{Z_1, Z_2, \dots, Z_d\}$ и множество ресурсов системы $E = \{E_1, E_2, \dots, E_m\}$, обеспечивающих ее функционирование и необходимых для удовлетворения потребностей СУ.

Исходные данные, характеризующие противоборствующую сторону: $N_{дв}$ – количество средств, предназначенных для обнаружения воздействия ДФ; $L_{дв}(n_{дв}, i)$ – множество средств, предназначенных для обнаружения воздействия ДФ $n_{дв}$, $n_{дв} = \overline{1, N_{дв}}$ находящихся на i -м, $i \in N_y$ узле (элементе) СС; $\lambda_{дв}(n_{дв}, \lambda_{n_{дв}})$ – множество, характеризующее интенсивность воздействия ДФ на элементы СС, определяемое по воздействию на средства обнаружения воздействия в виде интенсивности потока $\lambda_{n_{дв}}$ от $n_{дв}$ -го средства.

Исходные данные, характеризующие достоверность (α) и точность (ε) моделирования.

Показатели и критерии, ограничения и допущения, принятые в методике:

Показатель: вероятность нарушения устойчивого функционирования СС.

Критерий: $P_{наруш\ функ} \leq P_{наруш\ функ\ зад}$; $t_{уст\ функ} > T_{функ\ зад}$.

Допущения и ограничения:

- на период функционирования (моделирования) СС ее структура задана и остается неизменной;
- воздействия, приводящие к нарушению структуры СС, т.е. удаление УС и линий связи не рассматривается;
- узлы СС способны выполнить весь перечень заданных функций и задач;
- пропускная способность линий связи между узлами СС, линий привязки элементов СС и других систем известна и позволяет системе выполнять свое целевое предназначение;
- передача сообщений пользователей между узлами осуществляется по известному алгоритму. Для передачи сообщений в СС выбирается кратчайший маршрут, включающий минимальное количество промежуточных узлов;

- СС имеет ограниченный ресурс, позволяющий варьировать параметрами элементов;
- не рассматривается восстановление работоспособности СС из состояния полного разрушения системы.

Область применения: методика применима для ситуаций нарушения функционирования сложных технических систем, таких как системы и сети связи, информационные системы, информационно-телекоммуникационные системы, качество и эффективность выполнения которых определяются требованиями к ним.

Последовательность проведения расчетов по методике. Как следует из принятых ограничений и допущений, СС функционирует с выполнением требований, предъявляемых к ней. На нее осуществляется воздействие различных ДФ, приводящих к нарушению процесса функционирования системы, т.е. невыполнению задач и функций системы.

Последовательность применения разработанной методики обеспечения ФУ СС состоит из этапов, представленных на рисунке 1. На первом этапе производится ввод исходных данных. Далее разрабатывается структурно-функциональная модель СС, позволяющая определять ее возможности по выполнению функций и задач СС и СУ.

На втором этапе осуществляется контроль выполнения профиля функционирования СС. На третьем этапе проверяется наличие конфликтов в системе. При обнаружении конфликта, обусловленного отличием профиля процесса функционирования СС от профиля функционирования СС, причины возникновения конфликта определяют на четвертом этапе.

Под профилем функционирования системы понимается характеристика системы, характеризующая ее потребность в выполнении целевого предназначения системы, определяемого взаимосвязанным выполнением целей, функций, задач и требований, предъявляемых к системе. В работе профиль функционирования системы соответствует профилю плана и обозначается Q .

Профиль процесса функционирования системы – характеристика процесса функционирования системы показывающая в любой момент времени степень достижения целевого предназначения системы, выполнения профиля функционирования системы, а также количество выполненных и выполняемых целей, функций, задач, требования, предъявляемых к системе и ее элементам. В работе обозначается Q_p .

На пятом этапе проверяется, обусловлен ли конфликт отсутствием ресурса для выполнения текущего профиля без его изменения (возможность выполнения текущего профиля функция СС

существующей структурой системы). Если нет, то на 6 этапе проверяется возникновение конфликта из-за появления новой задачи, функции, что определяет потребность изменения профиля функционирования СС. На 7 этапе определяется потребный ресурс СС для выполнения новой задачи, функции. Если да, то на 8 этапе определяются функции и задачи текущего профиля функционирования СС, которые будут не выполнены из-за отсутствия ресурса для них.

На 9 этапе оценивается необходимость синтеза СС сначала по функциональному предназначению, потом по структуре системы.

При отсутствии необходимости синтеза СС на 10 этапе используется ресурс из резерва или ресурсы, запланированные для выполнения других задач, функций, которые в данный момент не задействованы для выполнения других задач, функций.

На 11 этапе, при необходимости, осуществляют синтез СС для обеспечения выполнения задач, функций.

На 12 этапе изменяют профиль функционирования СС и предоставляют информацию о произведенном синтезе системы и измененном профиле на этапе 1, где корректируются исходные данные для системы.

При достижении требуемого (заданного) времени функционирования СС на этапе 13 оценивают необходимость дальнейшего контроля СС.

Порядок осуществления синтеза СС, соответствующий блоку 11 рисунка 1, включает этапы, представленные на рисунке 2, которые рассмотрим ниже.

Действия, выполняемые в блоке 1, соответствуют первому этапу методики. Исходные данные формируются в системе контроля процесса функционирования СС и поступают в базу данных, где формируются характеристики профиля процесса функционирования СС и профиля функционирования СС.

В блоке 2 на основании применения структурно-функциональной модели СС, применения методов формирования профиля СС, модели контроля процесса функционирования СС и методики контроля процесса функционирования системы, осуществляется формирование профилей и контроль выполнения профиля функционирования СС.

В блоке 3 осуществляется сравнение профилей. Если условие выполняется, то продолжается контроль выполнения профиля, если условие не выполняется, и профили не соответствуют, то в блоке 4 определяют причину несоответствия профилей.

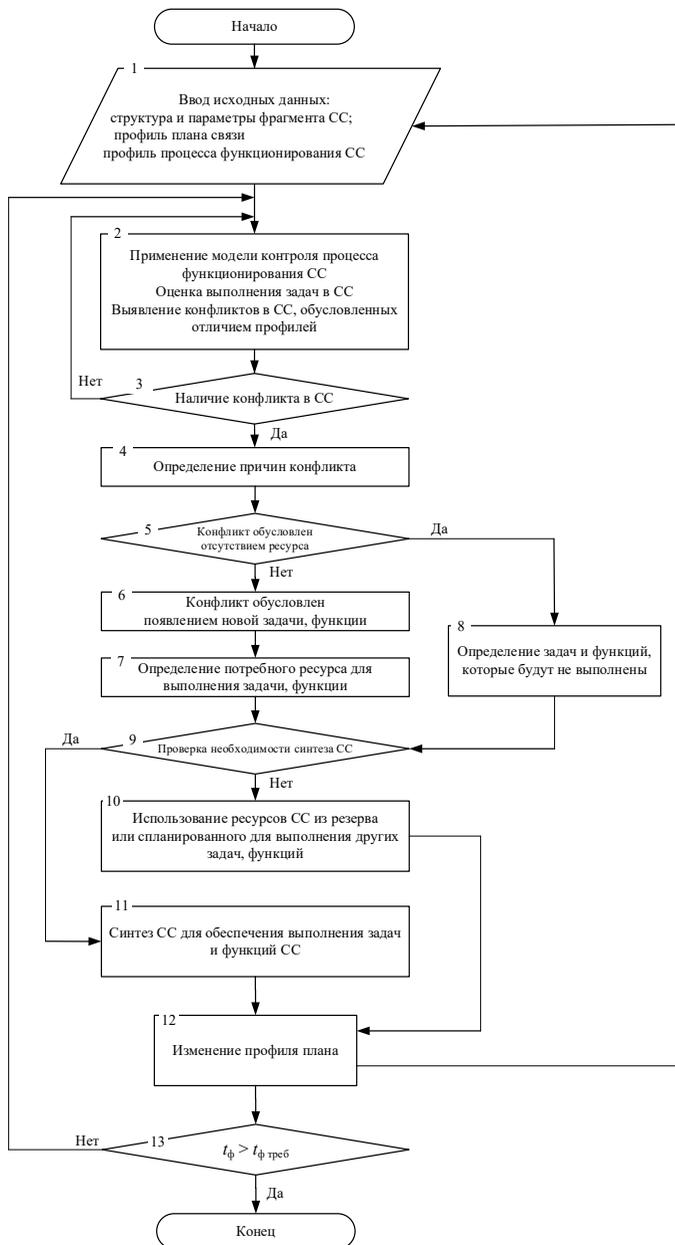


Рис. 1. Блок-схема последовательности применения методики

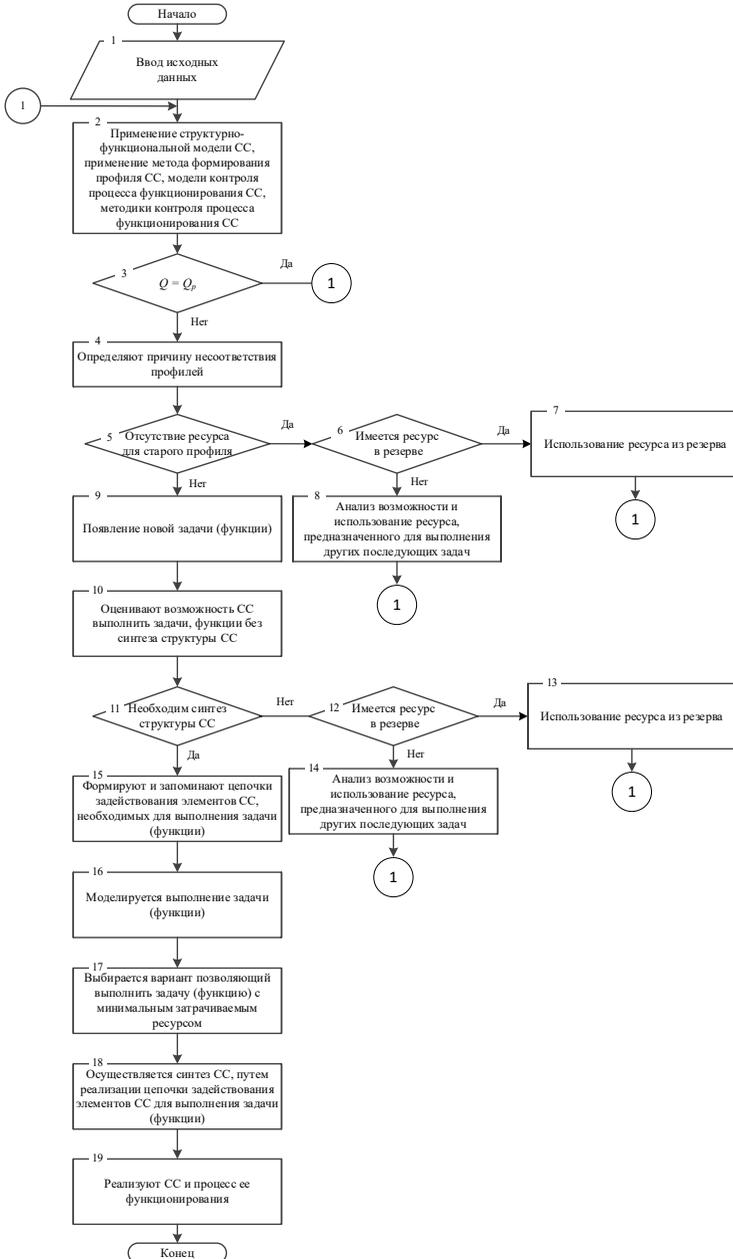


Рис. 2. Блок-схема синтеза СС для обеспечения ФУ

В блоке 5 проверяется наличие ресурса для выполнения профиля функционирования СС. Если ресурс отсутствует, то в блоке 6 проверяется наличие требуемого ресурса в резерве. Если в резерве ресурс есть, то он используется в блоке 7 для выполнения профиля функционирования СС. В противном случае используется ресурс, предназначенный для выполнения других задач в блоке 8.

Если ресурс имеется для выполнения текущего профиля функционирования СС, а конфликт обусловлен появлением новой задачи, функции блок 9, то оценивается возможность СС выполнить ее новую задачу, функцию без синтеза структуры СС блок 11.

Если необходимости синтеза структуры нет, то в блоке 12 проверяется наличие ресурса в резерве для выполнения новой задачи, функции. Если резерв имеется, переходим к блоку 13 и используем его для выполнения новой задачи, функции, если он отсутствует, то переходим к блоку 14 – анализируется возможность использования ресурса, предназначенного для выполнения других последующих задач, функций, и при наличии такой возможности он используется.

Если присутствует необходимость синтеза СС, то переходят к блоку 15, где формируют и запоминают варианты (цепочки) использования элементов СС, для выполнения новой задачи, функции.

В блоке 16 моделируется выполнение цепочкой элементов новой задачи, функции.

В блоке 17 выбирается вариант задействования элементов СС, позволяющий выполнить задачу, функцию с минимальными затратами ресурсов.

В блоке 18 осуществляется синтез СС путем реализации цепочек задействования ее элементов для выполнения новой задачи, функции. После получения необходимых данных их запоминают и реализуют функционирование СС (блок 19).

2. Определение интенсивности синтеза СС и ее элементов в условиях появления конфликтов в ней. Определение интенсивности синтеза СС в разработанной методике выполнено с помощью математической модели, описывающей процесс функционирования СС, который может быть представлен в виде графа состояний СС (рисунок 3).

Под интенсивностью синтеза СС понимается характеристика перехода системы из текущего функционально устойчивого состояния в другое функционально устойчивое состояние, которое позволяет обеспечить реализацию целевого предназначения СС.

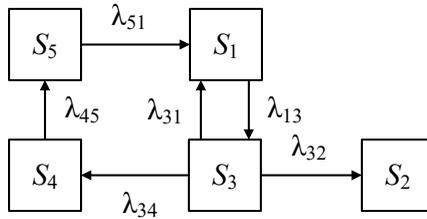


Рис. 3. Граф состояний СС

На рисунке 3, ребра графа показывают переходы из одной вершины в другую, которые в графе отображают состояния процесса функционирования системы.

Предлагается рассмотреть пять состояний СС (S_1 - S_5), описание которых представлено в таблице 1. Рассмотренное множество состояний представляет собой полную группу событий. Каждое состояние характеризуется условиями функционирования СС в любой момент времени. Процесс перехода из одного состояния в другое обусловлен особенностями и характером рассматриваемого процесса функционирования СС.

Таблица 1. Дискретные состояния графа состояний СС

№ п/п	Состояние	Процессы, характеризующие состояние СС	Входящий поток	Исходящий поток
1	S_1	Требования, предъявляемые к СС выполняются в процессе ее функционирования, обеспечиваются заданные требования по ФУ. Формируется профиль функционирования СС и профиль процесса функционирования СС в процессе контроля функционирования СС.	$\lambda_{31}, \lambda_{51}$	λ_{13}
2	S_2	Прекращение устойчивого функционирования СС	λ_{32}	
3	S_3	Выявление системой контроля конфликта, обусловленного отличием профилей	λ_{13}	$\lambda_{31}, \lambda_{32}, \lambda_{34}$
4	S_4	Формирование вариантов устранения конфликта (формирование нового профиля плана), моделирование процесса функционирования СС в соответствии с новым вариантом профиля плана	λ_{34}	λ_{45}
5	S_5	Синтез СС в соответствии с новым профилем плана и полученными данными моделирования	λ_{45}	λ_{51}

Процесс формирования графа, представленного на рисунке 3, показан на рисунке 4. Его можно описать с помощью двух состояний (рисунок 4(а)), которые показывают, что система либо функционально устойчива, т.е. выполняются заданные показатели функциональной устойчивости (состояние 1), или устойчивость функционирования системы связи снижена до недопустимого уровня (состояние 2), т.е. происходит отклонение характеризующих ее показателей ниже области допустимых значений. Нарушение функционирования системы обусловлено воздействием различных ДФ независимо от их природы. Результатом такого воздействия является отсутствие у системы возможности выполнить необходимый перечень задач и функций (состояние 3) (рисунок 4(б)), что характеризуется конфликтом невозможности выполнения профиля функционирования СС. При нарушении функционирования СС (возникновении конфликта) необходимо обеспечить переход СС из состояния 2 в 1. В данном случае предлагается рассмотреть два дополнительных состояния: формирование вариантов устранения конфликта (формирование нового профиля плана), моделирование функционирования СС в соответствии с новым профилем плана (состояние 4) и преобразования СС в соответствии с ним – состояние синтеза СС (состояние 5) (рисунок 4(в)).

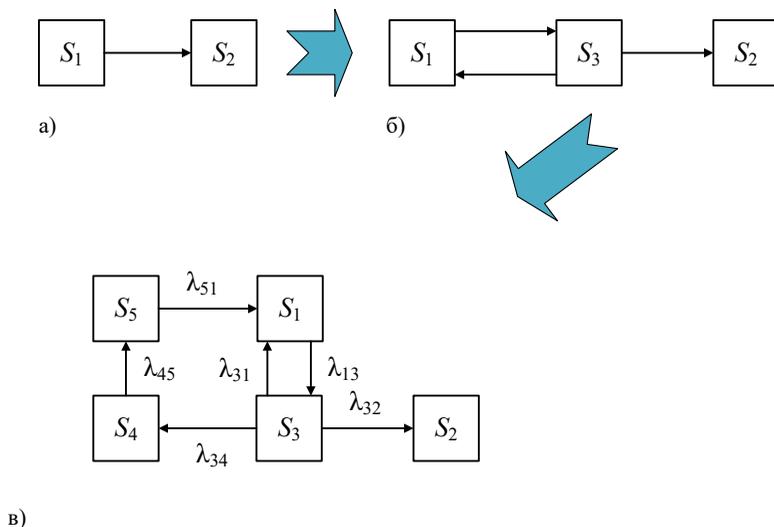


Рис. 4. Логика построения графа, представленного на рисунке 3

Корректность и адекватность представленной модели основана на ее соответствии общим закономерностям функционирования систем.

Оценка эффективности функционирования СС с возможностью синтеза ее для обеспечения ФУ связана с необходимостью моделирования в режиме реального времени. Это обуславливает целесообразность использования математического аппарата Марковских случайных процессов, необходимое условие которого – потоки событий являются простейшими, т. е. обладают свойствами стационарности, ординарности и не имеют последствий [34].

Возникновение конфликтов и переход из одного состояния в другое является случайным процессом, поэтому процесс функционирования СС, описываемый графом, представленным на рисунке 3, можно представить, как Марковский случайный процесс с дискретными состояниями и непрерывным временем [34, 35].

Процесс перехода из одного состояния системы в другое происходит под действием потоков событий, которые описываются интенсивностями λ_{ij} . Для описания процесса функционирования СС рассмотрим следующий перечень потоков событий:

λ_{13} – поток заявок воздействия на СС различных дестабилизирующих факторов – интенсивность возникновения конфликтов в СС;

λ_{32} – поток заявок при невозможности выполнения функций и задач – переход в нерабочее состояние;

λ_{31} – поток заявок после воздействия дестабилизирующих факторов на переход в функционально устойчивое состояние (воздействие на СС ДФ не привело к нарушению ее устойчивого функционирования);

λ_{14} – поток заявок на формирование возможных вариантов устранения конфликта и нового профиля функционирования СС, моделирование возможных вариантов устранения конфликта и нового профиля;

λ_{45} – поток заявок на синтез СС в соответствии с одним из вариантов устранения конфликта и новым профилем функционирования СС (профилем плана);

λ_{51} – поток заявок на переход СС в функционально устойчивое состояние.

Использование предложенной модели способствует поиску необходимых значений интенсивностей синтеза СС, при возникновении конфликтов в ней, обусловленных воздействием ДФ,

что позволит обеспечить достижение системой своего целевого предназначения.

Для различных сценариев состояния системы в условиях воздействия ДФ СС переходит из текущего состояния S_j в состояние S_j (поток интенсивностей λ_{ij}), которое может характеризоваться конфликтом.

Пусть первоначально моделируемая СС находится в состоянии, в котором обеспечивается ее ФУ в соответствии с заданными требованиями – S_1 . Процесс перехода из данного устойчивого состояния в другое – неустойчивое, обусловлен изменением обстановки, в которой она функционирует.

В соответствии с графом состояний СС (рисунок 3) переход ее в функционально устойчивое состояние может происходить в следующих случаях:

- воздействия ДФ, не приводящих к конфликту в системе. При этом она переходит в ФУ состояние, которое определяется нахождением значений параметров, характеризующих состояние системы, в пределах заданной нормы. Такое состояние можно рассматривать, как ситуацию устранения воздействия ДФ и определения возможности обеспечения ФУ СС без необходимости синтеза системы и формирования нового профиля плана (замена элемента системы, ресурса, взятого из резерва или ресурса, спланированного для другой задачи). Переход в такое состояние происходит под действием потока заявок λ_{31} ;

- осуществления синтеза системы в соответствии с профилем функционирования СС, необходимого для устранения возникшего конфликта в системе, после соответствующих этапов моделирования. Переход в такое состояние происходит под действием потоков заявок λ_{34} , λ_{45} , λ_{51} .

Нарушение функционирования СС, обусловленное возникновением конфликта и (или) не выполнением требований, предъявляемых к ней, влечет переход системы из состояния выявления конфликта в состояние поиска вариантов его устранения и моделирования функционирования системы (формирования нового профиля плана). Переход в такое состояние происходит под воздействием потока заявок λ_{43} .

Обеспечение процесса устойчивого функционирования системы в пределах требуемого интервала значений параметров, характеризующих выполнение требований, предъявляемых к СС, осуществляется путем изменения интенсивности потоков заявок на

переход системы из состояния обнаружения конфликта в состояния ее моделирования и синтеза.

В процессе функционирования системы происходит измерение параметров, характеризующих процессы, происходящие в ней в соответствии с алгоритмом (рисунок 2). Формируется множество вариантов устранения конфликта, моделируется функционирование системы с использованием таких вариантов в состоянии S_4 , после чего происходит измерение значений параметров, характеризующих функционирование СС и выбор оптимального варианта ее синтеза. В состоянии S_5 осуществляется синтез системы, в соответствии с профилем плана, что под действием потока заявок λ_{51} позволяет перевести систему в функционально устойчивое состояние.

Интенсивность изменения параметров зависит от активности воздействия ДФ, интенсивности и количества возникающих конфликтов в СС, а также возможностей СС по реализации профиля плана.

Для описания процесса функционирования СС, представленного графом на рисунках 3 и 4, необходимо разработать математическую модель функционирования СС.

В рассматриваемом случае СС в любой момент времени может находиться в одном из состояний S_1, S_2, \dots, S_5 или переходить из одного состояния в другое. Под вероятностью i -го состояния будем понимать такую вероятность $p_i(t)$, для которой СС в момент времени t будет находиться в S_i состоянии. Согласно [36] для рассматриваемого графа составляются уравнения Колмогорова – линейные дифференциальные уравнения (ЛДУ) с неизвестными функциями $p_i(t)$:

$$\left\{ \begin{array}{l} \frac{dp_1(t)}{dt} = \lambda_{31}p_3(t) + \lambda_{51}p_5(t) - \lambda_{13}p_1(t); \\ \frac{dp_2(t)}{dt} = \lambda_{32}p_3(t); \\ \frac{dp_3(t)}{dt} = \lambda_{13}p_1(t) - (\lambda_{31} + \lambda_{32} + \lambda_{34})p_3(t); \\ \frac{dp_4(t)}{dt} = \lambda_{34}p_3(t) - \lambda_{45}p_4(t); \\ \frac{dp_5(t)}{dt} = \lambda_{45}p_4(t) - \lambda_{51}p_5(t); \\ \sum_{i=1}^5 p_i(t) = 1. \end{array} \right. \quad (2)$$

Выбор начальных условий определяется исходя из возможных состояний СС. Начальное состояние описывается вектором вероятностей начальных состояний Марковской цепи:

$$p_i(0) = \left((1 - P_{\text{наруш функц}}) P_{\text{наруш функц}} \ 0 \ 0 \ 0 \right). \quad (3)$$

Задавая численные значения интенсивностей λ (таблица 1) и переходя к непрерывному времени $t \rightarrow \infty$, решается система ЛДУ (2) с постоянными коэффициентами (однородный Марковский процесс). Для любого момента времени сумма всех вероятностей состояний системы равна единице:

$$\sum_{i=1}^5 p_i(t) = 1. \quad (4)$$

Значения интенсивностей заявок определяются в соответствии с требованиями, заданными стратегиями моделирования, выбираемыми в зависимости от исходных данных.

Постановка задачи на моделирование:

Требуется оценить вероятность обеспечения функциональной устойчивости процесса функционирования СС в зависимости от интенсивностей возникновения конфликтов в ней.

Исходные данные:

- множество рассматриваемых состояний СС;
- уравнения Колмогорова (2), характеризующие функционирование рассматриваемой системы;
- вектор вероятностей начальных состояний СС (3), описываемой графом (рисунок 3);
- нормировочное условие (4);
- интенсивности потока событий, соответствующие сценариям моделирования СС.

Решения задач для системы ЛДУ можно разделить на три группы [36]: приближенно-аналитические методы; графические или машинно-графические методы; численные методы.

Численные методы предполагают получение приближенных значений p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0; t_1]$. Применение к полученной числовой таблице значений p_i способа аппроксимации, например, сплайн-интерполяции, позволяет иметь приближенное решение $p(t)$ на заданном интервале времени, что по сравнению с другими методами решения, позволяет решать

поставленную прикладную задачу и оценивать ее возможности [35, 37].

Недостатки методов Эйлера и других численных методов решения более высоких порядков [36, 38], заключающиеся в необходимости вычисления на каждом шаге частных производных функции $S(t, p)$, что приводит к большой вычислительной сложности, предопределили выбор в качестве решения системы ЛДУ классического метода – метода Рунге-Кутта четвертого порядка с фиксированным шагом интегрирования, имеющего вид (5), где h – приращение, соответствующее шаговой поправке Эйлера, Δp_i – средневзвешенная величина поправок $h\eta^1_i, h\eta^2_i, h\eta^3_i, h\eta^4_i$ каждого этапа интегрирования (с весовыми коэффициентами 1/6, 2/6, 2/6, 1/6 соответственно), то есть результат усреднения с указанными коэффициентами четырехэтапных поправок [37].

Первый этап соответствует применению явного метода Эйлера, второй и третий – уточненных методов Эйлера, а четвертый – неявного метода. Геометрическое толкование метода известно [37]:

$$\begin{cases} \eta_1^i = S(t_i, p_i); \\ \eta_2^i = S(t_i + h/2, p_i + \eta_1^i \cdot h/2); \\ \eta_3^i = S(t_i + h/2, p_i + \eta_2^i \cdot h/2); \\ \eta_4^i = S(t_i + h, p_i + \eta_3^i \cdot h); \\ \Delta p_i = (\eta_1^i + 2\eta_2^i + 2\eta_3^i + \eta_4^i) \cdot h/6; \\ p_{i+1} = p_i + \Delta p_i. \end{cases} \quad (5)$$

Использование метода Рунге-Кутта обусловлено тем, что для решения (2) применение методов Эйлера и исключения не позволяет решить данное уравнение из-за необходимости решения уравнения, связывающего функции $p_i(t)$ вместе.

Приводим систему (2) к векторному представлению – столбец D , где каждый элемент соответствует правой части определенного дифференциального уравнения в системе:

$$D(t, p) = \begin{cases} \lambda_{31}p_3(t) + \lambda_{51}p_5(t) - \lambda_{13}p_1(t); \\ \lambda_{32}p_3(t); \\ \lambda_{13}p_1(t) - (\lambda_{31} + \lambda_{32} + \lambda_{34})p_3(t); \\ \lambda_{34}p_1(t) - \lambda_{45}p_4(t); \\ \lambda_{45}p_4(t) - \lambda_{51}p_5(t). \end{cases} \quad (6)$$

Используя известный [37, 38] порядок решения системы ЛДУ методом Рунге-Кутты, учитывая вектор вероятностей начальных состояний $p_i(0)$, интервал интегрирования $[t_0; t_1]$ и число этапов интегрирования n , производится расчет для заданных значений интенсивностей событий $\lambda_{ij} = \text{const}$ (Марковский однородный процесс) (таблица 2). Это позволит получить приближенные значения p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0; t_1]$ (таблица 3).

Таблица 2. Стратегии моделирования процесса функционирования СС

Интенсивность потока событий	λ	Значения интенсивностей потоков событий для стратегии										
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
интенсивность воздействия на СС ДФ, характеризующая возникновение в ней конфликта	λ_{13}	1	10	10	50	50	50	100	100	100	100	100
интенсивность перехода в состояние планирования синтеза и моделирования устранения конфликта	λ_{34}	0	0	5	0	10	10	0	0	10	20	30
интенсивность перехода в состояние синтеза системы	λ_{45}	0	0	5	0	10	10	0	0	10	20	30
интенсивность перехода в рабочее состояние после синтеза СС или ее элемента	λ_{51}	0	0	5	0	10	10	0	0	10	20	30
интенсивность, характеризующая переход СС в ФУ состояние, в котором отсутствует необходимость синтеза СС	λ_{31}	1	9	9	45	45	40	99	90	90	90	90
интенсивность перехода в функционально неустойчивое состояние, когда конфликт устранить не получается	λ_{32}	0	1	1	5	5	10	1	10	10	10	10

Для получения приближенных решений $p(t)$ на заданном интервале времени используем сплайн-интерполяцию к полученной числовой таблице значений p_i .

Для оценки ФУ процесса функционирования СС в любой момент времени (шаге модельного времени) при различных стратегиях, характеризующих возникновение конфликтов в системе (таблица 2), предлагается использовать метод, который позволяет получить вероятностно-временные характеристики, описывающие состояния СС в условиях воздействия ДФ и возникновения конфликтов в ней.

Таблица 3. Приближенные решения $p_i(t)$

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$				
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$
1	t_0	$p_1(t_0)$	$p_2(t_0)$	$p_3(t_0)$	$p_4(t_0)$	$p_5(t_0)$
...
n	t_1	$p_1(t_1)$	$p_2(t_1)$	$p_3(t_1)$	$p_4(t_1)$	$p_5(t_1)$

На основе формального описания процесса функционирования СС получаем вероятность нарушения функционирования СС $P_{\text{нарушфункц}} = p_2(t)$.

Требуется оценить функциональную устойчивость предлагаемой модели, описывающей процесс функционирования СС для различных сценариев (исходных данных). Зададим граничные значения в различных стратегиях функционирования взаимодействующих сторон.

Для примера рассмотрим стратегию С2 и исходные данные для нее. Определяем интервал интегрирования $t_0 = 0, t_1 = 1$ и число этапов интегрирования $n = 1000$. Выбор интервала и этапов определяется точностью и быстродействием проводимого исследования, а также потребностями исследователя. Далее в соответствии со стратегией С2 осуществляется векторное представление выражения (2), где каждый элемент соответствует правой части дифференциального уравнения в системе с заданными интенсивностями:

$$D(t, p) = \begin{pmatrix} 9p_3(t) + 0p_5(t) - 10p_1(t); \\ 1p_3(t); \\ 10p_1(t) - (9 + 1 + 0)p_3(t); \\ 0p_1(t) - 0p_4(t); \\ 0p_4(t) - 0p_5(t). \end{pmatrix} \quad (7)$$

Производим расчет по методу Рунге-Кутты со средневзвешенной величиной поправок каждого этапа интегрирования (5) и получаем приближенные значения p_i на интервале с фиксированным шагом интегрирования 10^{-3} (таблица 4).

Таблица 4. Приближенные значений $p_i(t)$ для стратегии С2

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$				
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$
1	0,001	0.99	$4.967 \cdot 10^{-6}$	$9.901 \cdot 10^{-3}$	0	0
2	0,002	0.98	$1.974 \cdot 10^{-5}$	0.02	0	0
3	0,003	0.971	$4.411 \cdot 10^{-5}$	0.029	0	0
...
999	0,999	0.299	0.385	0.316	0	0
1000	1,000	0.299	0.385	0.315	0	0

Применяя к полученной числовой таблице значений p_i способ аппроксимации (сплайн-интерполяции), получаем приближенное решение $p(t)$ на заданном интервале времени. Графики зависимостей вероятностей состояний процесса функционирования СС $p_1(t), p_2(t), \dots, p_5(t)$ для значений интенсивностей событий, соответствующие стратегии С2 (таблица 2), представлены на рисунке 5.

Характер выявленных зависимостей (рисунок 5) говорит о том, что система еще не достигла стационарного состояния. При этом низкая интенсивность воздействия ДФ и возникновения конфликтов в СС позволяет ей оставаться в функционально устойчивом состоянии.

На основании представленного выше примера, для всех остальных стратегий функционирования СС (таблица 2), рассчитываются вероятностные и временные характеристики для соответствующих интенсивностей.

Получаем приближенные значения p_i на интервале $t \in [t_0; t_1]$ с фиксированным шагом интегрирования 10^{-3} для значений интенсивностей потоков событий, соответствующих стратегиям С1, С3 – С11 (увеличение интенсивности воздействия ДФ и появления конфликтов в СС (таблица 2), сплайн-интерполяция значений которых представлена на графиках зависимостей вероятностей состояний от времени (рисунки 6 – 15).

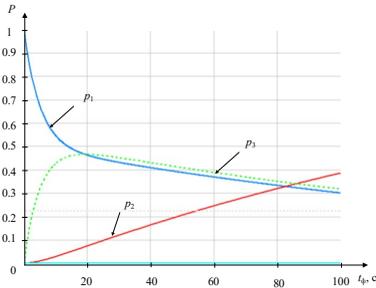


Рис. 5. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией C2

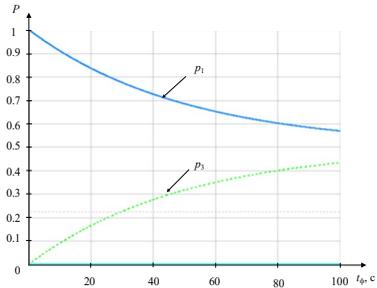


Рис. 6. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией C1

Характер выявленных зависимостей (рисунки 6, 7) говорит о том, что система, аналогично сценарию C2, еще не достигла стационарного состояния. При этом низкая интенсивность воздействия ДФ и возникновения конфликтов в СС позволяет системе связи оставаться в функционально устойчивом состоянии. Рассмотрим поведение системы при увеличении интенсивности на переход в моделирование и синтез СС.

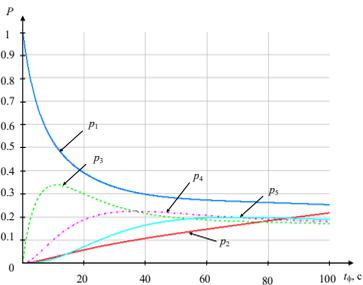


Рис. 7. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией C3

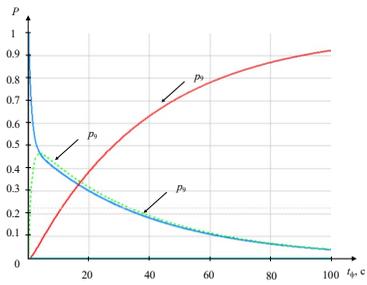


Рис. 8. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией C4

Характер выявленных зависимостей (рисунок 8) говорит о том, что система, аналогично сценариям C1, C2, C3 еще не достигла стационарного состояния. Время нарушения устойчивого функционирования системы связи с вероятностью $P_{\text{нарушфункц}} = 0,7$ составляет 480 ед. модельного времени. Далее рассмотрим увеличение

интенсивностей синтеза системы при сохранении интенсивностей перехода в нерабочее состояние. Видно (рисунок 9), что с увеличением интенсивностей на синтез системы время устойчивого функционирования СС с вероятностью $P_{\text{нарушфункц}} = 0,7$ увеличивается и составляет 985 ед. модельного времени. Рассмотрим случай увеличения интенсивности перехода в функционально неустойчивое состояние. С увеличением интенсивностей отказов (рисунок 10), обусловленных конфликтами и воздействиями ДФ время нарушения устойчивого функционирования СС с вероятностью $P_{\text{нарушфункц}} = 0,7$ уменьшается и составляет 458 ед. модельного времени.

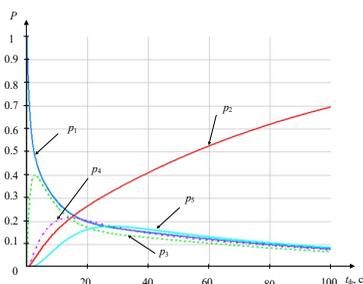


Рис. 9. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С5

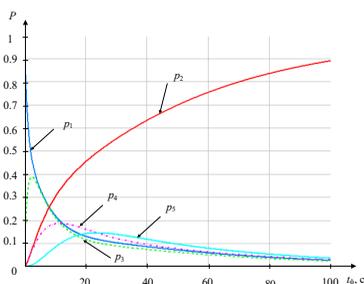


Рис. 10. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С6

При увеличении интенсивности воздействия на систему ДФ и возникновения большего количества конфликтов без синтеза системы получены зависимости, характер которых (рисунок 11) говорит о том, что система, аналогично сценариям С1 и С2, еще не достигла стационарного состояния. При этом на всем времени моделирования система является функционально устойчивой.

Увеличение интенсивности воздействия на систему ДФ приводит к возникновению большего количества конфликтов, а также увеличению интенсивностей перехода в нерабочее состояние (рисунок 12). Характер полученных зависимостей показывает, что система не достигла стационарного состояния. При этом с увеличением интенсивностей отказов, обусловленных конфликтами и воздействиями ДФ, время нарушения устойчивого функционирования СС с вероятностью $P_{\text{нарушфункц}} = 0,7$ составляет 240 ед. модельного времени.

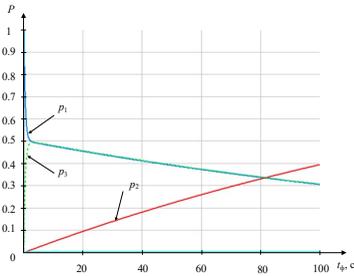


Рис. 11. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С7

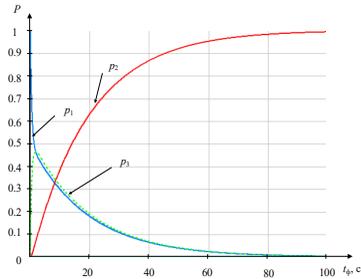


Рис. 12. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С8

Рассмотрим поведение системы при дальнейшем увеличении интенсивности перехода в состояния моделирования и синтеза СС с последующим переходом в функционально устойчивое состояние.

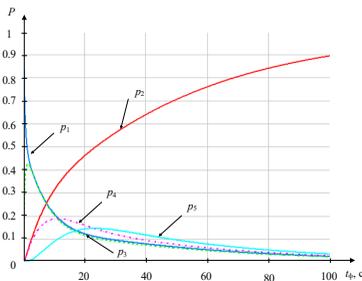


Рис. 13. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С9

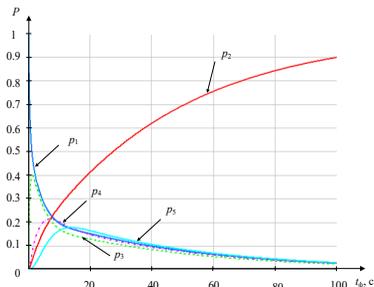


Рис. 14. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С10

При увеличении интенсивности воздействия на систему ДФ и, вследствие этого, возникновении большего количества конфликтов, а также увеличении интенсивностей перехода в состояния моделирования и синтеза СС получены зависимости, характер которых (рисунок 13) показывает, что с увеличением интенсивностей перехода в состояние синтеза и возвращения в функционально устойчивое состояние СС время нарушения ее устойчивого функционирования с вероятностью $P_{\text{нарушфункц}} = 0,7$ составляет 492 ед. модельного времени,

что говорит об эффективной работе системы контроля и восстановления работоспособности системы и ее элементов.

При увеличении интенсивности перехода в состояния моделирования и синтеза СС получены зависимости, характер которых (рисунок 14) говорит о том, что с увеличением интенсивностей перехода в состояние синтеза и возвращения в функционально устойчивости состояние СС время нарушения устойчивого функционирования СС с вероятностью $P_{\text{нарушфункц}} = 0,7$ составляет 509 ед. модельного времени, что говорит об эффективной работе системы контроля и восстановления работоспособности системы и ее элементов.

Таким образом, дальнейшее увеличение интенсивностей потоков событий на моделирование и синтез СС при сохраняющихся интенсивностях потока событий воздействия ДФ и возникновения конфликтов закономерно приводит к снижению вероятности нарушения функционирования СС (рисунок 15). Время нарушения устойчивого функционирования СС с вероятностью $P_{\text{нарушфункц}} = 70\%$ составляет 521 ед. модельного времени.

Изменение интенсивностей заявок соответствует изменению стратегий взаимодействующих сторон и, как следствие, изменению вероятности нарушения функционирования СС (таблица 5). Гистограмма зависимости представлена на рисунке 16.

Таблица 5. Сводная таблица показателей функциональной устойчивости СС

№	Интенсивность воздействия ДФ, характеризующая возникновение конфликтов	Интенсивность возникновения неустраиваемых конфликтов в СС	Интенсивность синтеза СС	Вероятность нарушения функционирования $P_{\text{нарушфункц}}$ ($t\phi = 80 \text{ с}$)	Среднее время устойчивого функционирования СС $P_{\text{нарушфункц}} < 70 \%$
C1	1	0	0	0	> 1000
C2	10	1	0	0.319	> 1000
C3	10	1	5	0.182	> 1000
C4	50	5	0	0.868	480
C5	50	5	10	0.619	> 1000
C6	50	10	10	0.835	503
C7	100	1	0	0.329	> 1000
C8	100	10	0	0.983	240
C9	100	10	10	0.842	492
C10	100	10	20	0.84	509
C11	100	10	30	0.838	521

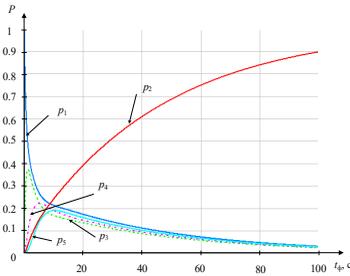


Рис. 15. Расчет вероятностей нахождения системы в моделируемых состояниях в соответствии со стратегией С11

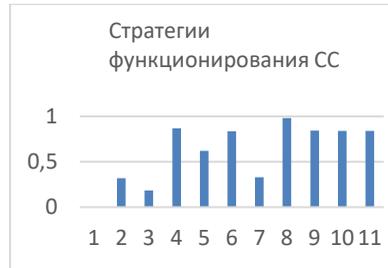


Рис. 16. Гистограмма зависимости вероятности нарушения устойчивого функционирования СС от стратегии ее функционирования

Разработанная модель процесса функционирования СС в условиях воздействия различных ДФ, обуславливающих возникновение конфликтов в СС, учитывает влияние и интенсивность возникновения в ней конфликтов. Процесс обеспечения ФУ СС сводится к поиску стратегии синтеза СС в зависимости от интенсивности воздействия ДФ, приводящей к увеличению времени функционирования СС с заданной допустимой вероятностью ФУ.

Как видно из таблицы 5 и рисунка 16 с увеличением интенсивности возникновения конфликтов в СС вероятность нарушения устойчивого функционирования падает. При этом при равных условиях низкая интенсивность перехода в неработоспособное состояние СС позволяет обеспечить более длительное нахождение системы в функционально устойчивом состоянии.

С увеличением интенсивности возникновения перехода в режимы моделирования и синтеза системы с последующим переходом в режим устойчивого функционирования вероятность нарушения устойчивого функционирования падает, а время устойчивого функционирования СС увеличивается. При этом при равных условиях низкая интенсивность перехода в неработоспособное состояние СС позволяет обеспечить более длительное нахождение системы связи в функционально устойчивом состоянии.

Модель функционирования СС, как составная часть методики обеспечения функциональной устойчивости СС, за счет выявления конфликтов в СС, выполнения синтеза СС и ее элементов, позволяет определить зависимость процесса устойчивого функционирования СС от механизма моделирования (планирования), синтеза СС и ее

элементов. Кроме этого, оценивать эффективность системы контроля процесса функционирования СС и обоснованно выбирать алгоритмы обеспечения функциональной устойчивости.

4. Заключение. Количество ДФ, влияющих на функционирование, как отдельных элементов СС, так и всей системы, с каждым годом растет. Это связано, в первую очередь, с появлением новых средств воздействия у злоумышленников, совершенствованием их тактико-технических характеристик. Успешность реализации таких воздействий зависит от многих факторов, например, характера воздействия, средств и квалификации злоумышленника, используемой в СС системы защиты и контроля и т.д. В результате таких воздействий может нарушаться устойчивость функционирования СС, что недопустимо для критически важных объектов.

С целью уменьшения вероятности нарушения ФУ СС разработана методика обеспечения функциональной устойчивости СС в условиях воздействия ДФ, основанная на выявлении конфликтов в СС, обусловленных несоответствием профиля процесса функционирования СС профилю функционирования СС.

Практическая значимость методики заключается в том, что она позволяет выявлять зависимость времени устойчивого функционирования СС с заданной вероятностью от интенсивности перехода в состояние синтеза СС и ее элементов и интенсивности воздействия ДФ, появления конфликтов в СС, иными словами, определять время устойчивого функционирования СС.

Разработанная методика обеспечения функциональной устойчивости СС может использоваться лицами, принимающими решение, и должностными лицами, которые занимаются планированием связи, при решении расчетных задач, в ходе оценки обстановки и разработки предложений по управлению связью.

Полученные результаты являются основой и определяют наиболее перспективные направления для разработки подходов по обеспечению ФУ СС в условиях воздействия ДФ различной природы в ходе построения, модернизации и наращивании системы связи, а также при планировании связи.

Литература

1. Кондрашов Ю.В., Сатдинов А.И., Синюк А.Д., Остроумов О.А. Концептуальная модель контроля функций системы связи для выявления конфликтных ситуаций // Т-Comm – Телекоммуникации и транспорт. 2022. Т. 16. № 5. С. 21–27. DOI: 10.36724/2072-8735-2022-16-5-21-27.
2. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. // СПб.: Научное издание, 2020. 337 с.

3. Остроумов О.А. Проблема обеспечения функциональной устойчивости систем критически важных объектов // Электросвязь. 2022. № 1. С. 38–42. DOI: 10.34832/ELSV.2022.26.1.005.
4. Тарасов А.А. Функциональная реконфигурация отказоустойчивых систем: монография // М.: Логос. 2012. 152 с.
5. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С. 16–21.
6. Остроумов О.А. Модель контроля функционирования системы связи // Известия Тульского государственного университета. Технические науки. 2022. № 3. С. 300–309.
7. Лаута О.С., Баленко Е.Г., Федоров В.Х., Лепешкин О.М., Остроумов О.А. Метод построения профиля функционирования сложной технической системы // Инженерный вестник Дона. 2023. № 2(98). С. 48–77. URL: ivdon.ru/magazine/archive/n1y2023/8183. (дата обращения: 26.10.2023).
8. El-Mowafy A. On detection of observation faults in the observation and position domains for positioning of intelligent transport systems // Journal of Geodesy. 2019. vol. 93. no. 10. pp. 2109–2122. DOI: 10.1007/s00190-019-01306-1.
9. Zhang Y., Wang L., Xiang Y., Ten C.-W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations // IEEE Transactions on Smart Grid. 2015. vol. 6. no. 4. pp. 1707–1721. DOI: 10.1109/TSG.2015.2396994.
10. Falahati B., Fu Y. Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies // IEEE Transactions on Smart Grid. 2014. vol. 5. no. 4. pp. 1677–1685. DOI: 10.1109/TSG.2014.2310742.
11. Falahati B., Fu Y., Wu L. Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies // IEEE Transactions on Smart Grid. 2012. vol. 3. no. 3. pp. 1515–1524. DOI: 10.1109/TSG.2012.2194520.
12. Haring I., Ebenhoch S., Stolz A. Quantifying Resilience for Resilience Engineering of Socj Technical Systems // European Journal for Security Research. 2016. vol. 1. pp. 21–58. DOI: 10.1007/s41125-015-0001-x.
13. Brauner F., Claben M., Fiedrich F. Competence as Enabler of Urban Critical Infrastructure Resilience Assessment // Urban Disaster Resilience and Security: Addressing Risks in Societies. 2018. pp. 171–184. DOI: 10.1007/978-3-319-68606-6_11.
14. Грудинин И.В., Суровикин С.В. Управление ресурсами информационно-управляющей подсистемы АСУ огнем в интересах обеспечения ее живучести // Известия Института инженерной физики. 2016. № 3(41). С. 57–62.
15. Pashintsev V.P., Chipigs A.F., Koval S.A., Skorik A.D. Analytical method for determining the interval of spatial correlation of fading in single-beam decameter radio line // Telecommunications and Radio Engineering. 2021. vol. 80. no. 2. pp. 89–104. DOI: 10.1615/TelecomRadEng.2021038432.
16. Савищенко Н.В. Остроумов О.А. Расчет оптимального и рационального числа ветвей разнесения в каналах связи с аддитивным белым гауссовым шумом и общими замираниями Райса-Накагами // Информационно-управляющие системы. 2015. № 6(79). С. 71–80. DOI: 10.15217/issn1684-8853.2015.6.71.
17. Петренко С.А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. 2009. Т. 41. С. 175–193.
18. Kotenko I., Saenko I., Lautu O., Karpov M. Methodology for management of the protection system of smart power supply networks in the context of cyberattacks // Energies. 2021. vol. 14(18). no. 5963. DOI: 10.3390/en14185963.

19. Haque M.A., Shetty S., Krishnappa B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019. pp. 273–281. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
20. Haque M.A., De Teyou G.K., Shetty S., Krishnappa B. Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights, IEEE International Conference on Intelligence and Security Informatics (ISI). 2018. pp. 25–30. DOI: 10.1109/ISI.2018.8587398.
21. Zhu Q. Multilayer Cyber-Physical Security and Resilience for Smart Grid // Smart Grid Control, Power Electronics and Power Systems. 2019. pp. 225–239. DOI: 10.1007/978-3-319-98310-3_14.
22. Kete N., Punzo G., Linkov I. Enhancing resilience within and between critical infrastructure systems // Environment Systems and Decisions. 2018. vol. 38. pp. 275–277. DOI: 10.1007/s10669-018-9706-5.
23. Alsubaie A., Alutaibi K., Marti J. Resilience Assessment of Interdependent Critical Infrastructure // Critical Information Infrastructures Security: 10th International Conference, CRITIS. 2016. pp. 43–55. DOI: 10.1007/978-3-319-33331-1_4.
24. Bologna S., Fasani A., Martellini M. Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures // Cyber Security: Deterrence and IT protection for critical infrastructures. Cham: Springer International Publishing, 2013. pp. 57–72.
25. Hammad A.W.A., Haddad A. Infrastructure Resilience: Assessment, Challenges and Insights // Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer. Cham, 2021. pp. 1–13. DOI: 10.1007/978-3-319-71059-4_25-1.
26. Saaty T.L. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process // RACSAM-Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. SerieA. Matemáticas. 2008. vol. 102. pp. 251–318.
27. Бородакий Ю.В., Тарасов А.А. О Функциональной устойчивости информационно-вычислительных систем // Известия ЮФУ. Технические науки. 2006. Т. 62. № 7. С. 5–12.
28. Богатырев В.А. К повышению надежности вычислительных систем на основе динамического распределения функций // Изв. Вузов СССР. Приборостроение. 1981. Т. 24. № 8. С. 62–65.
29. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. The Probability of Timely Redundant Service in a Two-Level Cluster of a Flow of Requests that is Heterogeneous in Functionality and Allowable Delays // International Conference on Distributed Computer and Communication Networks. Cham: Springer Nature Switzerland, 2022. pp. 122–134.
30. Турута Е.Н. Организация распределения задач в вычислительных системах, обеспечивающая их отказоустойчивость // Автоматика и вычислительная техника. 1985. № 1. С. 5–14.
31. Турута Е.Н. Обеспечение отказоустойчивости многопроцессорных систем путем перераспределения задач отказавших модулей // Системы управления информационных сетей. М.: Наука, 1983. С. 187–198.
32. Машков О.А., Гостев В.И., Машков В.А. Межмодульный обмен диагностической информацией при самодиагностировании сложных систем // Кибернетика и вычислительная техника. 1996. № 105. С. 108–118.

33. Королев А.Н. Функциональная устойчивость навигационно-информационных систем // Известия вузов. Приборостроение. 2018. Т. 61. № 7. С. 559–565. DOI: 10.17586/0021-3454-2018-61-7-559-565.
34. Портенко Н.И., Скороход А.В., Шуренко В.М. Марковские процессы // Итог науки и техники. Современные проблемы математики. Фундаментальные направления. 1989. Т. 46. С. 5–245.
35. Кузьмич А.А., Лепешкин О.М., Пермяков А.С. Модель функционирования системы телекоммуникационной связи в условиях информационного противоборства // Радиолокация, навигация, связь: Сборник трудов XXVIII Международной научно-технической конференции, посвященной памяти Б.Я. Осипова (г. Воронеж, 27-29 сентября 2022): в 6 т. Воронеж: Издательский дом ВГУ, 2022. С. 203–211.
36. Вержбицкий В.М. Численные методы (математический анализ и обыкновенные дифференциальные уравнения): Учеб. пособие для вузов. М.: Высш. шк., 2001. 382 с.
37. Иванов И.И. Модель функционирования распределенных информационных систем при использовании маскированных каналов связи // Системы управления, связи и безопасности. 2020. № 1. С. 198–234. DOI: 10.24411/2410-9916-2020-10107.
38. Тихонов В.И., Миронов М.А. Марковские процессы. М.: Сов. Радио, 1977. 488 с.

Лепешкин Олег Михайлович — д-р техн. наук, доцент кафедры, кафедра «безопасности инфотелекоммуникационных систем специального назначения», Военная орден Жукова и Ленина краснознаменная академия связи имени С.М. Буденного (ВАС). Область научных интересов: безопасность сетей связи, безопасность социотехнических систем, защита информации. Число научных публикаций — 158. lereshkin1@yandex.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +7(812)247-9832.

Остроумов Олег Александрович — канд. техн. наук, докторант кафедры, кафедра «безопасности инфотелекоммуникационных систем специального назначения», Военная орден Жукова и Ленина краснознаменная академия связи имени С.М. Буденного (ВАС). Область научных интересов: криптографическая защита информации, передаваемой по открытым каналам связи, обеспечение безопасности критически важных объектов систем связи и управления. Число научных публикаций — 134. oleg-26stav@mail.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +7(812)247-9832.

Михайличенко Николай Валерьевич — канд. техн. наук, доцент кафедры, кафедра «программной инженерии и вычислительной техники», Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруневича (СПбГУТ). Область научных интересов: автоматизированные системы управления, построение центров обработки данных. Число научных публикаций — 69. 23esn2008@ Rambler.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +79111758475.

Пермяков Александр Сергеевич — канд. техн. наук, доцент кафедры, кафедра «безопасности инфотелекоммуникационных систем специального назначения», Военная орден Жукова и Ленина краснознаменная академия связи имени С.М. Буденного (ВАС). Область научных интересов: защита систем и сетей связи. Число научных публикаций — 56. Permyak.as@ya.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +7(812)247-9832.

O. LEPESHKIN, O. OSTROUMOV, N. MIKHAILICHENKO, A. PERMYAKOV
**A METHOD FOR ENSURING THE FUNCTIONAL STABILITY OF
A COMMUNICATION SYSTEM BY DETECTING CONFLICTS**

Lepeshkin O., Ostroumov O., Mikhailichenko N., Permyakov A. A Method for Ensuring the Functional Stability of a Communication System by Detecting Conflicts.

Abstract. Introduction: Modern complex technical systems are often critical. Criticality is due to the consequences of disruption of the functioning of such systems, and their failure to fulfill the required list of functions and tasks. The process of control and management of such systems is carried out using communication systems and networks that become critical for them. There is a need to ensure the stable functioning of the complex technical systems themselves, their control and monitoring systems, communication systems and networks. The paper proposes a method for ensuring the functional stability of a communication system, the basis of which is the process of identifying and eliminating conflicts in it due to the difference between the profile of functioning and the profile of the process of functioning of the system. The proposed model of the process of functioning of the communication system allows, based on changes in the intensity of the impact on the system of destabilizing factors, the identification of conflicts and their elimination, to determine the probability of ensuring the functional stability of the system. The purpose of the study: to develop a methodology for ensuring the functional stability of a communication system under the influence of destabilizing factors and the emergence of conflicts, a model of the process of the system's functioning, which makes it possible to determine the probability of the system being in a functionally stable state. Methods of graph theory and matrix theory, the theory of Markov processes. Results: an approach is proposed for assessing the functional stability of a communication system under the influence of destabilizing factors, a technique has been developed to ensure the functional stability of a communication system. Practical significance: the results of the study can be used in the design and construction of complex technical systems, decision support systems, control, communication and management.

Keywords: functional stability, criticality, communication system, control system, complex technical system, system functioning profile, functions, tasks, regulations.

References

1. Kondrashov Yu.V., Satdinov A.I., Sinyuk A.D., Ostroumov O.A. [A conceptual model for monitoring the functions of a communication system for identifying conflict situations]. T-Comm – Telekommunikacii i transport – T-Comm – Telecommunications and transport. 2022. vol. 16. no. 5. pp. 21–27. DOI: 10.36724/2072-8735-2022-16-5-21-27. (In Russ.).
2. Makarenko S.I. Modeli sistemy svyazi v usloviyah prednamerennyh destabilizirujushhijh vozdeystvij i vedenija razvedki. Monografiya [Models of communication systems in conditions of deliberate destabilizing impacts and intelligence. Monograph]. St. Petersburg: Naukoemkie Tehnologii Publ., 2020. 337 p. (In Russ.).
3. Ostroumov O.A. [The problem of ensuring the functional stability of systems of critical facilities]. Elektrosvyaz– Telecommunications. 2022. no. 1. pp. 38–42. DOI: 10.34832/ELSV.2022.26.1.005. (In Russ.).
4. Tarasov A.A. Funktsional'naya rekonfiguratsiya otkazoustoychivykh sistem: monografiya [Functional reconfiguration of fault-tolerant systems: monograph]. Moscow: Logos, 2012. 152 p. (In Russ.).

5. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. [Technospheric warfare as the main way to resolve conflicts in the context of globalization]. *Voenaya misl' – Military Thought*. 2020. no. 10. pp. 16–21. (In Russ.).
6. Ostroumov O.A. A model for monitoring the functioning of a communication system. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskiye nauki – News of the Tula State University. Technical Sciences*. 2022. no. 3. pp. 300–309. (In Russ.).
7. Lauta O.S., Balenko E.G., Fedorov V.Kh., Lepeshkin O.M., Ostroumov O.A. [A method for constructing a profile of the functioning of a complex technical system]. *Inzhenernyj vestnik Dona – Don Engineering Bulletin*. 2023. no. 2(98). pp. 48–77. Available at: ivdon.ru/magazine/archive/n1y2023/8183. (accessed 26.10.2023). (In Russ.).
8. El-Mowafy A. On detection of observation faults in the observation and position domains for positioning of intelligent transport systems. *Journal of Geodesy*. 2019. vol. 93. no. 10. pp. 2109–2122. DOI: 10.1007/s00190-019-01306-1.
9. Zhang Y., Wang L., Xiang Y., Ten C.-W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. *IEEE Transactions on Smart Grid*. 2015. vol. 6. no. 4. pp. 1707–1721. DOI: 10.1109/TSG.2015.2396994.
10. Falahati B., Fu Y. Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies. *IEEE Transactions on Smart Grid*. 2014. vol. 5. no. 4. pp. 1677–1685. DOI: 10.1109/TSG.2014.2310742.
11. Falahati B., Fu Y., Wu L. Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies. *IEEE Transactions on Smart Grid*. 2012. vol. 3. no. 3. pp. 1515–1524. DOI: 10.1109/TSG.2012.2194520.
12. Haring I., Ebenhoch S., Stolz A. Quantifying Resilience for Resilience Engineering of Socij Technical Systems. *European Journal for Security Research*. 2016. vol. 1. pp. 21–58. DOI: 10.1007/s41125-015-0001-x.
13. Brauner F., Claben M., Fiedrich F. Competence as Enabler of Urban Critical Infrastructure Resilience Assessment. *Urban Disaster Resilience and Security: Addressing Risks in Societies*. 2018. pp. 171–184. DOI: 10.1007/978-3-319-68606-6_11.
14. Grudin I.V., Surovkin S.V. [Resource management of the information and control subsystem of the ACS by fire in the interests of ensuring its survivability]. *Izvestiya Instituta inzhenernoy fiziki– Bulletin of the Institute of Engineering Physics*. 2016. no. 3(41). pp. 57–62. (In Russ.).
15. Pashintsev V.P., Chipigs A.F., Koval S.A., Skorik A.D. Analytical method for determining the interval of spatial correlation of fading in single-beam decimeter radio line. *Telecommunications and Radio Engineering*. 2021. vol. 80. no. 2. pp. 89–104. DOI: 10.1615/TelecomRadEng.2021038432.
16. Savishchenko N.V. Ostroumov O.A. [Calculation of the optimal and rational number of diversity branches in communication channels with additive white Gaussian noise and common Rice-Nakagami fading]. *Informatsionno-upravliaiushchie sistemy – Information and control systems*. no. 6(79). 2015. pp. 71–80. DOI: 10.15217/issn1684-8853.2015.6.71. (In Russ.).
17. Petrenko S.A. [The concept of maintaining the efficiency of cyber systems under conditions of information and technical impacts]. *Trudy Instituta sistemnogo analiza Rossiyskoy akademii nauk – Proceedings of the Institute for System Analysis of the Russian Academy of Sciences*. 2009. vol. 41. pp. 175–193. (In Russ.).
18. Kotenko I., Saenko I., Lauta O., Karpov M. Methodology for management of the protection system of smart power supply networks in the context of cyberattacks. *Energies*. 2021. vol. 14(18). no. 5963. DOI: 10.3390/en14185963.
19. Haque M.A., Shetty S., Krishnappa B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. *IEEE 5th Intl Conference on Big Data Security*

- on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019. pp. 273–281. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
20. Haque M.A., De Teyou G.K., Shetty S. Krishnappa B. Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights, IEEE International Conference on Intelligence and Security Informatics (ISI). 2018. pp. 25–30. DOI: 10.1109/ISI.2018.8587398.
 21. Zhu Q. Multilayer Cyber-Physical Security and Resilience for Smart Grid. Smart Grid Control, Power Electronics and Power Systems. 2019. pp. 225–239. DOI: 10.1007/978-3-319-98310-3_14.
 22. Kete N., Punzo G., Linkov I. Enhancing resilience within and between critical infrastructure systems. Environment Systems and Decisions. 2018. vol. 38. pp. 275–277. DOI: 10.1007/s10669-018-9706-5.
 23. Alsubaie A., Alutaibi K., Marti J. Resilience Assessment of Interdependent Critical Infrastructure. Critical Information Infrastructures Security: 10th International Conference, CRITIS. 2016. pp. 43–55. DOI: 10.1007/978-3-319-33331-1_4.
 24. Bologna S., Fasani A., Martellini M. Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures. Cyber Security: Deterrence and IT protection for critical infrastructures. Cham: Springer International Publishing, 2013. pp. 57–72.
 25. Hammad A.W.A., Haddad A. Infrastructure Resilience: Assessment, Challenges and Insights. Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer. Cham, 2021. pp. 1–13. DOI: 10.1007/978-3-319-71059-4_25-1.
 26. Saaty T.L. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process. RACSAM-Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas. 2008. vol. 102. pp. 251–318.
 27. Borodaki Yu.V., Tarasov A.A. [On the Functional Stability of Information and Computing Systems]. Izvestiya YUFU. Tekhnicheskie nauki – Izvestiya SFedU. Technical science. 2006. vol. 62. no. 7. pp. 5–12. (In Russ.).
 28. Bogatyrev V.A. [To increase the reliability of computing systems based on the dynamic distribution of functions]. Izvestiya Vuzov SSSR. Priborostroenie – Izvestiya Vuzov USSR. Instrumentation. 1981. vol. 24. no. 8. pp. 62–65. (In Russ.).
 29. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. The Probability of Timely Redundant Service in a Two-Level Cluster of a Flow of Requests that is Heterogeneous in Functionality and Allowable Delays. International Conference on Distributed Computer and Communication Networks. Cham: Springer Nature Switzerland, 2022. pp. 122–134.
 30. Turuta E.N. [Organization of task distribution in computing systems, ensuring their fault tolerance]. Avtomatika i vychislitel'naya tekhnika – Automation and Computer Science. 1985. no. 1. pp. 5–14. (In Russ.).
 31. Turuta E.N. [Ensuring the fault tolerance of multiprocessor systems by redistributing the tasks of failed modules]. Sistemy upravleniya informatsionnyh setey – Control systems of information networks. M.: Nauka, 1983. pp. 187–198. (In Russ.).
 32. Mashkov O.A., Gostev V.I., Mashkov V.A. [Intermodule exchange of diagnostic information during self-diagnosis of complex systems]. Kibernetika i vychislitel'naya tekhnika – Cybernetics and Computer Science. 1996. no. 105. pp. 108–118. (In Russ.).
 33. Korolev A.N. [Functional stability of navigation and information systems]. Izvestiya vuzov. Priborostroenie – Izvestiya vuzov. Instrumentation. 2018. vol. 61. no. 7. pp. 559–565. DOI: 10.17586/0021-3454-2018-61-7-559-565. (In Russ.).

34. Portenko N.I., Skorokhod A.V., Shurenko V.M. [Markov processes]. Itog nauki i tehniki. Sovremennyye problemy matematiki. Fundamental'nye napravleniya – Results of science and technology. Modern problems of mathematics. Fundamental directions. 1989. vol. 46. pp. 5–245. (In Russ.).
35. Kuzmich A.A., Lepeshkin O.M., Permyakov A.S. [Model of functioning of the telecommunication system in the conditions of information confrontation] // Radiolokatsiya, navigatsiya, svyaz': Sborniktrudov XXVIII Mezhdunarodnoynauchno-tehnicheskoykonferentsii, posvyashchennoypamyati B.Ya. Osipova [Radar, navigation, communication: Proceedings of the XXVIII International scientific and technical conference dedicated to the memory of B.Ya. Osipov]. Voronezh: VSU Publishing House, 2022. pp. 203–211. (In Russ.).
36. Verzhbitsky V.M. Chislennyye metody (matematicheskyy analiz i obyknovennyye differentsial'nyye uravneniya): Ucheb. posobiye dlya vuzov [Numerical methods (mathematical analysis and ordinary differential equations): Proc. allowance for universities]. Moscow: Vysshaya shkola, 2001. 382 p. (In Russ.).
37. Ivanov I.I. [Model of functioning of distributed information systems when using masked communication channels]. Sistemy upravleniya, svyazi i bezopasnosti – Systems of Control, Communication and Security. 2020. no. 1. pp. 198–234. DOI: 10.24411/2410-9916-2020-10107. (In Russ.).
38. Tikhonov V.I., Mironov M.A. Markovskiye protsessy [Markov processes]. Moscow: Sov. Radio, 1977. 488 p. (In Russ.).

Lepeshkin Oleg — Ph.D., Dr.Sci., Associate professor of the department, Department protection of information and telecommunication systems for special purposes, Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after S.M. Budyonny (VAS). Research interests: security of communication networks, security of sociotechnical systems, information protection. The number of publications — 158. lepechkin1@yandex.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +7(812)247-9832.

Ostroumov Oleg — Ph.D., Doctoral student of the department, Department protection of information and telecommunication systems for special purposes, Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after S.M. Budyonny (VAS). Research interests: cryptographic protection of information transmitted through open communication channels, ensuring the security of communication and control systems critical objects. The number of publications — 134. oleg-26stav@mail.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +7(812)247-9832.

Mikhailichenko Nikolay — Ph.D., Associate professor of the department, Department of software engineering and computer science, St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Brunevich (SPbSUT). Research interests: automated control systems, building data centers. The number of publications — 69. 23esn2008@rambler.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +79111758475.

Permyakov Alexander — Ph.D., Associate professor of the department, Department protection of information and telecommunication systems for special purposes, Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after S.M. Budyonny (VAS). Research interests: protection of communication systems and networks. The number of publications — 56. Permyak.as@ya.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +7(812)247-9832.