КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ КОНТРОЛЯ ФУНКЦИЙ СИСТЕМЫ СВЯЗИ ДЛЯ ВЫЯВЛЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

Синюк Александр Демьянович,
Военная орденов Жукова и Ленина краснознаменная академия связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия, ***eentrop@rambler.ru***

Сатдинов Айрат Иршатович,
Военная орденов Жукова и Ленина краснознаменная академия связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия, ***sat-12@mail.ru***

Кондрашов Юрий Владимирович,
Военная орденов Жукова и Ленина краснознаменная академия связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия, ***kondrashov_30@mail.ru***

Остроумов Олег Александрович,
Военная орденов Жукова и Ленина краснознаменная академия связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия, ***oleg-26stav@mail.ru***

DOI: 10.36724/2072-8735-2022-16-5-21-27

Manuscript received 20 April 2022;
Accepted 16 May 2022

Ключевые слова: *функциональная устойчивость, критичность, система связи, система управления, функции, задачи, профиль, регламент*

Введение: **система связи является неотъемлемой частью любой системы управления, которая в своем составе имеет подсистемы диагностики, мониторинга и контроля ее состояния. Несовершенство современных средств контроля, диагностики и мониторинга приводит к ситуации, когда системы поддержки принятия решения и лица, принимающие решение, осуществляют свою деятельность в условиях неопределенности. Процесс принятия решения и реагирования на изменение состояния системы из-за воздействия различных факторов может привести к невыполнению системой своих задач. Для эффективного решения данной проблемы система управления должна постоянно иметь достоверную информацию о состоянии своих элементов, а система поддержки принятия решения по состоянию элементов прогнозировать процесс функционирования системы связи.** ***Цель исследования:*** **разработка подхода к контролю функционирования системы связи, позволяющего получать достоверную и своевременную информацию о контролируемом объекте, а также выявлять и своевременно реагировать на отклонения от устойчивого функционирования системы связи.** ***Методы:*** **использование процессного подхода и математического аппарата теории иерархических решений для формализации функционирования системы связи и формирования профиля системы связи.** ***Результаты*****: предложен подход описания системы связи, включающий задачи и функции системы. На основании потребностей систем связи и управления формируется профиль функционирования системы связи, который сравнивается с формируемым в процессе функционирования системы связи профилем процесса функционирования системы связи. Результаты сравнения показывают наличие конфликтов, обусловленных воздействием различных дестабилизирующих факторов, условиями меняющейся обстановки и управляющими воздействиями вышестоящей системы управления. Полученные результаты используются для формирования поля решений, необходимых лицам, принимающим решение.** ***Практическая значимость:*** **результаты исследования могут быть использованы при проектировании и построении систем контроля, диагностики и мониторинга состояния системы связи. Предложенный подход может использоваться для контроля выполнения задач, функций системы связи в процессе ее функционирования.**

Информация об авторах:
Александр Демьянович Синюк, *д.т.н., доцент, профессор кафедры Общепрофессиональных дисциплин Военной орденов Жукова и Ленина краснознаменная академии связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия*
Айрат Иршатович Сатдинов, *к.т.н., доцент кафедры Военных систем космической, радиорелейной, тропосферной связи и навигации Военной орденов Жукова и Ленина краснознаменная академии связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия*
Юрий Владимирович Кондрашов, *к.т.н., старший преподаватель кафедры Автоматизированных систем специального назначения Военной орденов Жукова и Ленина краснознаменная академии связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия*
Олег Александрович Остроумов, *к.т.н., докторант Военной орденов Жукова и Ленина краснознаменная академии связи имени маршала Советского союза С.М. Буденного, г. Санкт-Петербург, Россия*

Для цитирования:
Синюк А.Д., Сатдинов А.И., Кондрашов Ю.В., Остроумов О.А. Концептуальная модель контроля функций системы связи для выявления конфликтных ситуаций // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №5. С. 21-27.

For citation:
Sinyuk A.D., Satdinov A.I., Kondrashov Yu.V., Ostroumov O.A. (2022) Communication system functions control conceptual model for detecting conflict situations. *T-Comm*, vol. 16, no.5, pp. 21-27. (*in Russian*)

Введение

На современном этапе развития общества, техники, информационных технологий, потребности в информационных услугах возникает необходимость обеспечения устойчивого функционирования систем, предназначенных для передачи информации и предоставления услуг потребителям. Современные системы связи представляют собой сложные иерархические функционально-динамические построения с большим количеством связей. В условиях функционирования такие системы в режиме реального времени осуществляют выполнение возложенных на них задач, своих функций для достижения целевого предназначения системы. Невыполнение их приводит к невозможности предоставления требуемых потребителем услуг. Возрастает значимость, критичность всех системы и ее отдельных элементов, обеспечивающих выполнение целевого предназначения системы.

Проблема обеспечения функциональной устойчивости может быть решена своевременным выявлением критически важных и значимых объектов и процессов и предупреждением нарушений их функционирования, не выполнение. Традиционно устойчивость систем рассматривается в аспекте только надежности [1, 2, 3, 4], или живучести, или помехоустойчивости, или киберустойчивости [5, 6, 7]. Количественно, как правило, устойчивость систем связи оценивается через вероятность ее обеспечения, однако подходов к обеспечению устойчивости через анализ процессов функционирования и количественной оценки задач, функций, требований и целей нет.

Основная часть. Система связи является составной частью системы управления, и предназначена, в первую очередь, для обеспечения процесса управления, т. е. для предоставления всех видов услуг лицам, принимающим решение, необходимых для управления. Одной из важнейших составляющих системы связи является подсистема управления связью. В процессе функционирования системы связи, для обеспечения ее функциональной устойчивости подсистема управления, через систему контроля и мониторинга, осуществляет сбор и обработку информации о состоянии системы связи и реализует управляющие воздействия на нее.

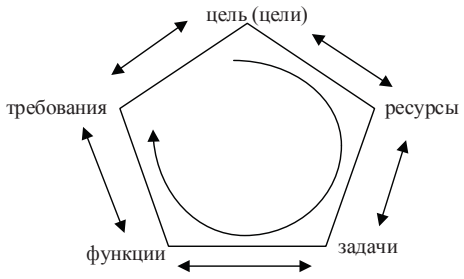

Рис. 1. Концептуальная модель обеспечения функционирования системы связи

Для описания функционирования системы связи рассмотрим модель, представленную на рис. 1. Для достижения целей система должна выполнять требования, обеспечиваемые выполнением возложенных на нее функций, задач и регламентов за счет имеющегося ресурса (маневра ресурсом), при этом для обеспечения быстродействия реагирования на нарушения функционирования элементов системы некоторые процессы должны быть автоматизированы. Отсутствие ресурса не выполнение функций, задач и регламентов, а также сбои в их выполнении, могут стать причиной нарушения ее устойчивого функционирования и не достижению целей системы.

Концептуальная модель представляет собой совокупность взаимосвязанных целей, требований, функций, задач и ресурсов системы. Системы связи представляет собой сложное иерархическое образование. Каждый нижестоящий уровень формируется исходя из требований вышестоящего и определяется набором соответствующих задач, функций, требований и целей. На самом нижнем уровне находятся ресурсы системы. Необходимость оценивания возможностей использования различных ресурсов систем представлена в работах [8-12]. К ресурсам можно отнести технику, персонал, время и т.д. Функционирование системы характеризуется значением $\{F_{\text{сист}}, F_{\text{сист треб}}\}$ и будет определяться, как:

$$F_{\text{сист}} = \{F_1, F_2, \ldots, F_n\},$$

где $F_n = \{F_n, F_{n\,\text{треб}}\}$, n – количество функций системы.

Управляющий элемент системы регулирует использование ресурсов, функция его определяется, как: $F_{\text{уэ}} = \{F_{\text{уэ}}, F_{\text{уэ треб}}(R)\}$. При рассмотрении модели функционирования системы связи необходимо учитывать связи между требованиями, функциями, задачами, подзадачами, а также влияние одних и тех же задач, функций, требований на различные элементы вышестоящей иерархии.

Главным для любой системы является обеспечение выполнения целевого предназначения. Цель (цели) системы связи может быть представлена в явном или не явном виде, при этом она, в первую очередь, будет определяться назначением системы, потребностями систем, лиц, в интересах которых функционирует система связи. Предназначение, цель, условия функционирования системы влияют на количество и качество дестабилизирующих факторов, влияние которых может привести к нарушениям, отказам, сбоям в системе.

Представленная на рисунке 1 модель состоит из совокупности взаимосвязанных множеств целей, требований, функций, задач и ресурсов:

$A = \{A_1, A_2, \ldots, A_a\}$ – множество целей системы, которые необходимо достигнуть в процессе функционирования системы связи. Цели формируются в виде требований, представляющих собой краткие и четкие формулировки, определяющих решение главной задачи системы связи, ее верхнего иерархического уровня;

$T = \{T_1, T_2, \ldots, T_n\}$ – множество требований к системе связи, соблюдение которых необходимо для ее устойчивого функционирования и достижения целей системы. Требования к системе связи определяют перечень функций системы, которые она должна выполнять для достижения целей системы связи;

$F = \{F_1, F_2, \ldots, F_c\}$ – множество функций, выполнение которых обеспечивает выполнение требований к системе связи. Каждая функция определяет перечень задач, решение которых способствует выполнению функций системы;

$Z = \{Z_1, Z_2, \ldots, Z_d\}$ – множество задач, обеспечивающих выполнение функций. В процессе функционирования системы связи, каждая задача может рассматриваться в виде регламента, определяемого пространственно-временным использованием ресурса системы, для выполнения задач;

$E = \{E_1, E_2, \ldots, E_d\}$ – множество ресурсов системы связи (находящихся в резерве и необходимых для выполнения задач системы связи).

Выполнение целей, требований, функций и задач будет представлять собой отображения:

$$P(R) \rightarrow P((A_k)_{k=1}^{n});$$
$$P(A_a) \rightarrow P((T_i)_{i=1}^{n});$$
$$P(T_n) \rightarrow P((F_j)_{j=1}^{c});$$
$$P(F_c) \rightarrow P((Z_q)_{q=1}^{d});$$
$$P(Z_d) \rightarrow P((E_m)_{m=1}^{e}),$$

где R – характеризует выполнение целевого предназначения системы.

Выполнение задачи представляет собой элементарное завершенное действие одного объекта s над другим v:

$$P(Z_d) \rightarrow P(s, v).$$

Анализ проблем функционирования и управления сложными системами [12-14] показал необходимость рассмотрения процесса функционирования системы связи, учитывающего не только воздействие различных дестабилизирующих факторов, но и процесс выполнения функций, задач и управления ресурсом системы [15-17]. Сложность описания функционирования сложных функционально-динамических систем заключается в необходимости мгновенного реагирования на нарушение функционирования любого из ее элементов, что затруднительно из-за большого количества элементов системы, связей между ними, часто сложных связей, а также динамики изменения условий их функционирования. Для описания функционирования системы связи, как процесса, необходимо рассматривать регламенты выполнения элементарных операций-задач. Совокупность регламентов задач формирует регламент функционирования всей системы. Качество и эффективность функционирования системы связи определяется выполнением регламентов и сравнением общего регламента с профилем системы связи.

В рамках ГОСТ Р 57628-2017 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» определяется необходимость разработки профилей защиты. Профилем защиты называется документ (информация), включающий проблему безопасности для объекта (совокупности объектов) и требования безопасности для устранения этой проблемы.

В международном стандарте ISO/IEC 15408 «Критерий оценки безопасности информационных технологий» под профилем защиты понимается документ, включающий в себя типовой набор требований, которым должны удовлетворять системы определенного класса.

Под профилем функционирования системы связи (рис. 2) будет пониматься документ (информация, правило), определяющий требования к устойчивому функционированию системы связи и правило выполнения данных требований, представляющее собой логическую взаимосвязь целей, требований, функций, задач, выполняемых системой связи и ресурсов, обеспечивающих их выполнение.

Каждая задача, функция, которые выполняет система связи в процессе функционирования, может быть представлена в виде регламента (рис. 3, 4).

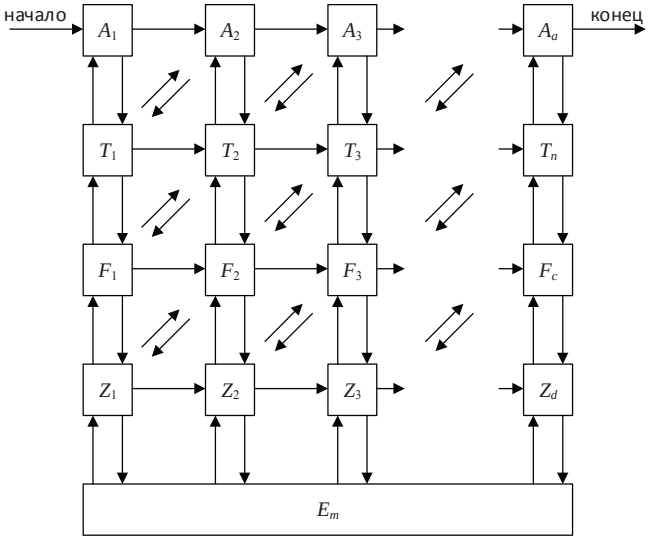

Рис. 2. Структура профиля функционирования системы связи

Под регламентом будет пониматься управленческий механизм, включающий перечисление и описание порядка выполнения профиля в установленные сроки и с использованием необходимого ресурса.

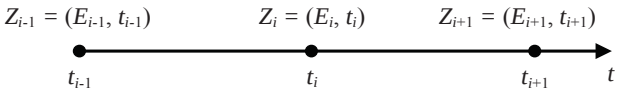

Рис. 3. Структура регламента задачи

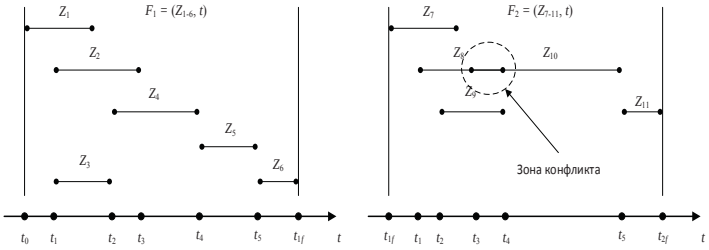

Рис. 4. Структура регламента функции

Для определения регламента выполнения системой своего функционального предназначения необходимо:

– исходя из целей и предназначения системы, определяются требования и целевая функция регламента;

– определить порядок выполнения регламента (реализации целей) для достижения конечного состояния системы;

– определить последовательность выполнения функций для обеспечения реализации целей и выполнения регламента;

– определить соотношение задач, функций и целей;

– производить анализ использования имеющегося ресурса.

Совокупность множеств целей, требований, функций, задач и ресурсов системы можно представить через профиль функционирования и регламент функционирования системы связи:

$$\{A, T, F, Z, E\},$$
$$\{A_p, T_p, F_p, Z_p, E_p\}.$$

Согласование уровней соответствующего профиля функционирования системы связи по вертикали и горизонтали на

этапе формирования системы связи для решения конкретной задачи будет способствовать выявлению конфликтных ситуаций между заданными требованиями к системе связи и обеспеченности выполнения их соответствующим ресурсом. Аналогично в процессе функционирования системы связи и контроля соответствия регламента профилю функционирования системы связи возможно выявление конфликтных ситуаций не соответствия регламента профилю, связанных с логической противоречивостью структуры регламента и выполнением процессов, действующих в системе связи. Причинами возникновения конфликтов функционирования СС может быть неправильное использование ресурсов системы, использование ресурсов системы, предназначенных для выполнения задачи, для другой задачи, отсутствие ресурса для обеспечения выполнения регламента, изменение (нарушение) последовательности и сроков выполнения задач, функций под действием управляющих воздействий вышестоящей системы управления, воздействием различных дестабилизирующих факторов.

Под конфликтом функционирования системы связи будет состояние системы связи (ее элементов), целей, требований, функций, задач, профили которых не соответствует соответствующему регламенту функционирования СС в данный момент времени.

Важное значение имеет возможность предсказания наступления конфликтов, исходя из информации получаемой системой в процессе мониторинга состояния системы связи и ее элементов и анализа предыдущей статистики возникновения неисправностей и конфликтов.

Под предиктивным контролем системы связи и ее элементов будет пониматься контроль, осуществляемый в режиме реального времени, который позволяет своевременно выявлять, а также прогнозировать наступление конфликтных ситуаций функционирования СС и обнаруживать критичность отдельных ее элементов за счет использования накопленной информации системы мониторинга состояния и функционирования системы связи и ее элементов.

Процесс мониторинга состояния системы и контроля выполнения профиля функционирования системы связи представляет собой последовательность определенных действий [18-20] (рис. 5).

На основе состав сил и средств системы связи, ее целей и задач, определенных вышестоящей системой формируется база данных, на основании которой формируются профили структуры системы связи и ее элементов, определяемые взаимосвязями между элементами системы, и профили функционирования, определяемые целями, требованиями, функциями и задачами системы. Сформированный профиль системы связи является неизменной величиной.

Кроме этого, при решении задачи обеспечения функционирования системы связи, предварительно и в процессе функционирования, производится:

– ранжирование, определение значимости или критичности объектов, задач, функций, требований, целей;

– при нарушении функционирования элементов системы, выявление их критичности [21] происходит резервирование ресурса для обеспечения объектов, задач, которые имеют большое значение, при отказе элемента (прекращении функционирования) системой осуществляется перераспределение ресурса системы, для обеспечения функционирования наиболее важных, значимых, критичных элементов системы, обеспечения выполнения цели, требований, функций и задач.

– использование нового ресурса, не задействованного в данный момент в выполнении задач системы и не планируемого для использования в задачах, функциях в ближайшее время. Длительность «ближайшего времени» определяется исходя из задач системы и указаниями должностных лиц, принимающих решение.

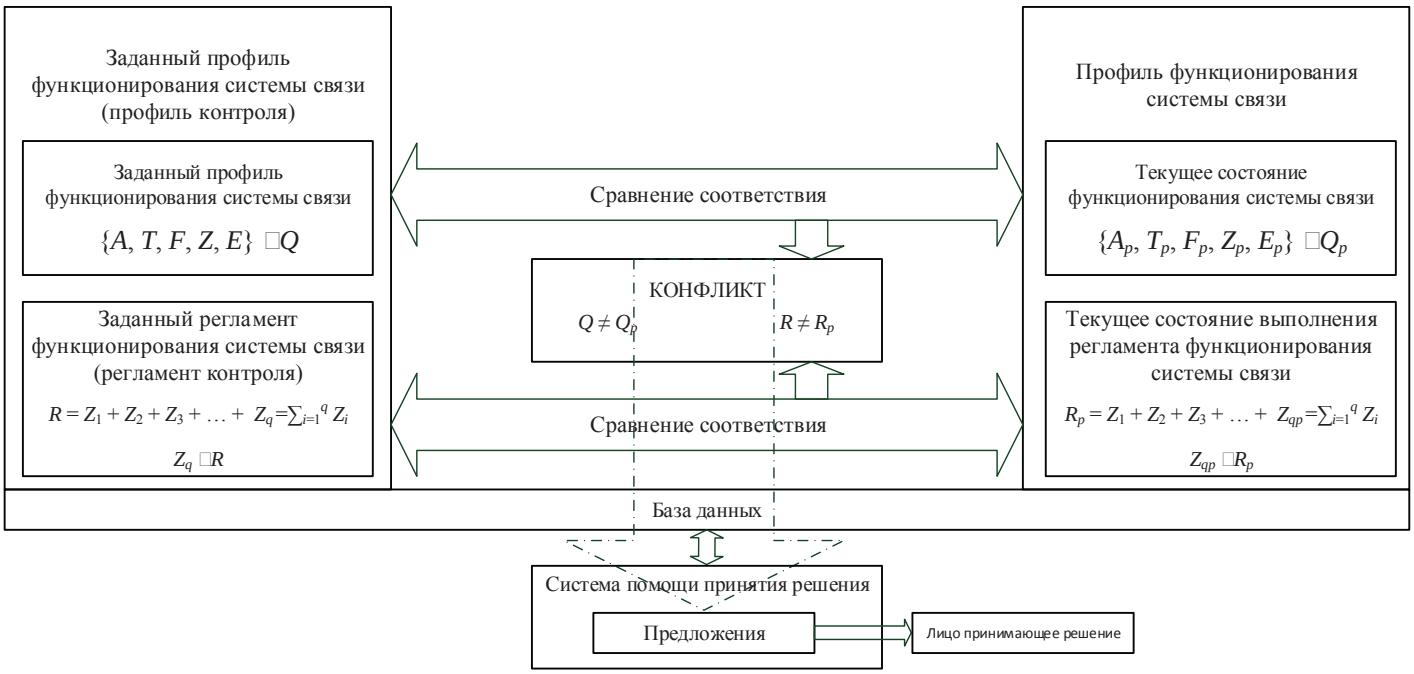

Рис. 5. Структура процесса контроля функционирования системы связи

В процессе функционирования системы происходит заполнение базы данных процессов, происходящих в системе связи (рис. 5). На основании полученных данных формируется регламент функционирования системы связи, основой которого являются регламенты выполнения простейших задач системы. Полученный системой контроля системы связи регламент функционирования сравнивается со сформированным профилем функционирования системы связи. Кроме этого, анализ выполнения регламента по вертикали и горизонтали позволяет производить контроль обеспеченности ресурсом целей, требований, функций и задач системы связи. Контроль обеспеченности ресурсом способствует выявлению критически важных задач и функций, а также элементов системы, обеспечивающих выполнение критически важных задач и функций.

При выявлении конфликтов (рис. 4) производится оценка ситуации и предоставляется информация о конфликте в систему помощи в принятии решения, которая формирует одно и более решений на устранение конфликта для системы управления связью. Параллельно система контроля предоставляет информацию вышестоящей системе управления о состоянии системы связи, выполняемых ее задачах и обеспеченности ресурсами. ЛПР на основании полученных данных о состоянии системы и выявленных конфликтах, а также информации, полученной от системы помощи в принятии решения, формируют управленческое воздействие на систему связи для ухода (устранения) от конфликта.

Заключение

Для обеспечения устойчивого функционирования системы связи необходимо постоянно проводить контроль ее состояния и функционирования. Для осуществления контроля система связи представляется в виде ее профиля, описывающего структуру и связи между элементами и выполняемые ее функции и задачи. В процессе функционирования системы формируется регламент функционирования, который сравнивается с профилем функционирования системы связи. При несоответствии регламента профилю и возникновении конфликта система обеспечивает уход от конфликта за счет использования маневра ресурсами и задачами.

Дальнейшим направлением исследования является поиск математических методов для описания процессов функционирования системы связи, выявления конфликтов в ней и разработки вербальной модели функционирования системы связи.

Литература

1. *Zhang Y., Wang L., Xiang Y., Ten C.-W.* Power System Reliability Evaluation With SCADA Cybersecurity Considerations // IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1707-1721, July 2015, doi: 10.1109/TSG.2015.2396994.

2. *Falahati B., Fu Y.* Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies // IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1677-1685, July 2014, doi: 10.1109/TSG.2014.2310742.

3. *Falahati B., Fu Y., Wu L.* Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies // IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515-1524, Sept. 2012, doi: 10.1109/TSG.2012.2194520.

4. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем. Спб.: Политехника, 2000. 248 с.

5. *Haring I., Ebenhoch S., Stolz A.* Quantifying Resilience for Resilience Engineering of Socij Technical Systems // Springer International Publishing. 2016. pp. 21-58. DOI: 10.1007/s41125-015-0001-x.

6. *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), Miami, FL, USA, 2018, pp. 25-30, doi: 10.1109/ISI.2018.8587398.

7. *Bologna S., Fasani A., Martellini M.* Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures // Cyber Security, pp. 57-72: Springer, 2013.

8. *Шостак Р.К., Новиков П.А., Лепешкин М.О., Худайназаров Ю.К.* Методика сетевого мониторинга защищенности узлов связи сети передачи данных от деструктивных программно-аппаратных воздействий // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. №2 (34). С. 301-304.

9. *Burlov V., Lepeshkin O., Lepeshkin M.* 2020 The synthesized model parameters of technosphere safety management in the region // E3S Web of Conferences, Topical Problems of Green Architecture, Civil and Environmental Engineering 2019 (TPACEE 2019) vol 164 07011 DOI: https://doi.org/10.1051/e3sconf/202016407011

10. *Лепешкин О.М., Шуравин А.С., Пермяков А.С., Зройчиков П.С., Шимаров Е.В.* Модель контроля информационной безопасности распределенной сети связи // Известия Тульского государственного университета. Технические науки. 2020. №12. С. 250-255.

11. *Петренко С.А.* Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий. Труды ИСА РАН. Т.41. 2009. С. 175-193.

12. *Дурняк Б.В., Машков О.А., Усаченко Л.М., Сабат В.И.* Методология обеспечения функциональной устойчивости иерархических организационных систем управления // Сборник научных статей: Институт проблем моделирования в энергетике, НАН Украины. В. 48. 2008. С. 3-21.

13. *Боговик А.В., Игнатов В.В.* Теория управления в системах военного назначения: Учеб. Спб.: ВАС, 2008. 460 с.

14. *Коцыняк М.А., Карпов М.А., Лаута О.С., Дементьев В.Е.* Управление системой обеспечения безопасности информационно-телекоммуникационной сети на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. 2020. №4. С. 3-10.

15. *Лепешкин О.М., Остроумов О.А., Савищенко Н.В.* Выполнение регламента процесса управления – критерий определения критичности системы // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей III Всероссийской научно-технической конференции. Анапа. 2021. С. 625-634.

16. *Лепешкин О.М., Остроумов О.А., Синюк А.Д.* Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. № 8. С. 109-114.

17. *Лепешкин О.М.* Синтез модели процесса управления социальными и экономическими системами на основе теории радикалов: автореферат диссертации на соискание ученой степени доктора технических наук. Санкт-Петербург, 2014. 35 с.

18. *Груздев Д.А., Закалкин П.В., Кузнецов С.И., Тесля С.П.* Мониторинг информационно-телекоммуникационных сетей // Труды учебных заведений связи. 2016. Т.2. №4. С. 46-50.

19. *Лепешкин О.М., Остроумов О.А., Черных И.С.* Система мониторинга и контроля функционального состояния критически важных объектов и объектов критической информационной инфраструктуры. Нейрокомпьютеры и их применение. Сборник тезисов докладов XIX Всероссийской научной конференции. Москва. 2021. С. 240-243.

20. *Пермяков А.С., Сташко Я.С.* Вопросы повышения защищенности информационно-телекоммуникационной сети на основе интеллектуализации // Нейрокомпьютеры и их применение XVIII Всероссийская научная конференция. Тезисы докладов. 2020. С. 226-227.

21. *Лепешкин О.М., Остроумов О.А., Черных И.С., Остроумов М.А.* К вопросу о понятии критически важного объекта // Проблемы технического обеспечения войск в современных условиях. Труды VI межвузовской научно-практической конференции. Санкт-Петербург. 2021. С. 17-20.

COMMUNICATION SYSTEM FUNCTIONS CONTROL CONCEPTUAL MODEL FOR DETECTING CONFLICT SITUATIONS

Alexander D. Sinyuk, *Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia,* ***eentrop@rambler.ru***
Airat I. Satdinov, *Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia,* ***sat-12@mail.ru***
Yury V. Kondrashov, *Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia,* ***kondrashov_30@mail.ru***
Oleg A Ostroumov, *Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia,* ***oleg-26stav@mail.ru***

Abstract
Introduction: a communication system is an integral part of any control system, which includes subsystems for diagnostics, monitoring and control of its condition. The imperfection of control modern means, diagnostics and monitoring leads to a situation where decision support systems and decision makers carry out their activities in conditions of uncertainty. The process of making a decision and responding to a change in the state of the system due to the influence of various factors can lead to the failure of the system to fulfill its tasks. To effectively solve this problem, the control system must constantly have reliable information about the state of its elements, and the decision support system for the state of the elements must predict the process of functioning of the communication system. *The purpose of the study*: to develop an approach to monitoring the functioning of the communication system, which allows obtaining reliable and timely information about the controlled object, as well as identifying and responding in a timely manner to deviations from the stable functioning of the communication system. *Methods*: using the process approach and the mathematical apparatus of the theory of hierarchical decisions to formalize the functioning of the communication system and form the profile of the communication system. *Results*: an approach for describing a communication system is proposed, including the tasks and functions of the system. Based on the needs of communication and control systems, a profile of the communication system functioning is formed, which is compared with the functioning process profile of the communication system formed in the process of the communication system functioning. The results of the comparison show the presence of conflicts caused by the influence of various destabilizing factors, the conditions of a changing environment and the control actions of a higher management system. The results obtained are used to form the field of decisions required by decision makers. *Practical significance*: the results of the study can be used in the design and construction of control systems, diagnostics and monitoring of the state of the communication system. The proposed approach can be used to control the fulfillment of tasks and functions of the communication system during its operation.

Keywords: *functional stability, criticality, communication system, control system, functions, tasks, profile, regulations.*

References

1. Y. Zhang, L. Wang, Y. Xiang and C. -W (2015). Ten Power System Reliability Evaluation With SCADA Cybersecurity Considerations. *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707-1721, July 2015, doi: 10.1109/TSG.2015.2396994
2. B. Falahati and Y. Fu (2014). Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies. *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1677-1685, July 2014, doi: 10.1109/TSG.2014.2310742
3. B. Falahati, Y. Fu and L. Wu (2012). Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies. *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1515-1524, Sept. 2012, doi: 10.1109/TSG.2012.2194520
4. I.A. Ryabinin (2000). Reliability and safety of structurally complex systems. St. Petersburg: Polytechnic. 248 p.
5. I. Haring, S. Ebenhoch, A. Stolz (2016). Quantifying Resilience for Resilience Engineering of Socij Technical Systems. *Springer International Publishing,* pp. 21-58. DOI: 10.1007/s41125-015-0001-x
6. M.A. Haque, G.K. De Teyou, S. Shetty and B. Krishnappa (2018). Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights. *IEEE International Conference on Intelligence and Security Informatics (ISI)*, Miami, FL, USA, pp. 25-30, doi: 10.1109/ISI.2018.8587398
7. S. Bologna, A. Fasani, and M. Martellini (2013). Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures. *Cyber Security*, pp. 57-72: Springer, 2013.
8. R.K. Shostak, P.A. Novikov, M.O. Lepeshkin, Yu.K. Khudainazarov (2019). Network monitoring methods of the data transmission network communication nodes security from destructive software and hardware influences. *Information technologies and systems: management, economics, transport, law*. No. 2 (34), pp. 301-304.
9. V. Burlov, O. Lepeshkin, M. Lepeshkin (2020). The synthesized model parameters of technosphere safety management in the region. *E3S Web of Conferences, Topical Problems of Green Architecture, Civil and Environmental Engineering 2019 (TPACEE 2019),* vol. 164 07011. DOI : https://doi.org/10.1051/e3sconf/202016407011

10. O.M. Lepeshkin, A.S. Shuravin, A.S. Permyakov, P.S. Zroichikov, E.V. Shimarov (2020). Model of information security control of a distributed communication network. *Proceedings of the Tula State University. Technical science*. No. 12, pp. 250-255.
11. S.A. Petrenko (2009). The concept of maintaining the efficiency of cyber systems in the conditions of information and technical influences. *Proceedings of the ISA RAS*. Vol. 41, pp. 175-193.
12. B.V. Durnyak, O.A. Mashkov, L.M. Usachenko, V.I. Sabat (2008). Methodology for ensuring the functional stability of hierarchical organizational management systems. *Collection of scientific articles: Institute for Modeling Problems in Energy, NAS of Ukraine*. Vol. 48, pp. 3-21.
13. A.V. Bogovik, V.V. Ignatov (2008). Control theory in military systems: Proc. SPb.: VAS. 460 p.
14. M.A. Kotsynyak, M.A. Karpov, O.S. Lauta, V.E. Dementiev (2020). The security system management of the information and telecommunication network based on the algorithms for the artificial neural network functioning. *Proceedings of the Tula State University. Technical science*. No. 4, pp. 3-10.
15. O.M. Lepeshkin, O.A. Ostroumov, N.V. Savishchenko (2021). Implementation of the regulation of the control process - a criterion for determining the criticality of the system. *State and prospects for the development of modern science in the direction of "Information security". Collection of articles of the III All-Russian Scientific and Technical Conference*. Anapa. 2021, pp. 625-634.
16. O.M. Lepeshkin, O.A. Ostroumov, A.D. Sinyuk (2021). Systematization of the fundamentals of the methodology for synthesizing the critical information infrastructure of the Russian Federation. *Military Thought*. No. 8, pp. 109-114.
17. O.M. Lepeshkin (2014). Synthesis of a model of the process of managing social and economic systems based on the theory of radicals: abstract of a dissertation for the degree of Doctor of Technical Sciences. St. Petersburg. 35 p.
18. D.A. Gruzdev, P.V. Zakalkin, S.I. Kuznetsov, S.P. Teslya (2016). Monitoring of information and telecommunication networks. *Proceedings of educational institutions of communication*. Vol. 2. No. 4, pp. 46-50.
19. O.M. Lepeshkin, O.A. Ostroumov, I.S. Chernykh (2021). System for monitoring and controlling the functional state of critical facilities and critical information infrastructure facilities. *Neurocomputers and their applications. Collection of abstracts of the XIX All-Russian scientific conference*. Moscow, pp. 240-243.
20. A.S. Permyakov, Ya.S. Stashko (2020). Issues of increasing the security of an information and telecommunication network based on intellectualization. *Neurocomputers and their application XVIII All-Russian Scientific Conference. Abstracts of reports*, pp. 226-227.
21. O.M. Lepeshkin, O.A. Ostroumov, I.S. Chernykh, M.A. Ostroumov (2021). To the question of the concept of a critically important object. *Problems of technical support of troops in modern conditions. Proceedings of the VI interuniversity scientific-practical conference*. St. Petersburg, pp. 17-20.

Information about authors:

Alexander D. Sinyuk, *Doctor of Technical Sciences, Associate Professor, General Professional Disciplines Department Professor of the Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia*

Airat I. Satdinov, *PhD, Associate Professor of the Department of Military Systems of Space, Radio Relay, Tropospheric Communications and Navigation of the Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia*

Yury V. Kondrashov, *PhD., Senior Lecturer of the Department of Automated Systems for Special Purposes of the Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia*

Oleg A. Ostroumov, *PhD., doctoral student of the Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia*