АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ В МАШИНОСТРОЕНИИ

УДК 355.358.1

УСТОЙЧИВОСТЬ РАСПРЕДЕЛЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ С УЧЕТОМ МОДЕЛИ ПРОГНОЗИРОВАНИЯ ПОСЛЕДСТВИЙ НЕПРЕДНАМЕРЕННЫХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

© 2024 г. А. М. Попов[1, *], В. И. Филатов[2, **]

[1]*Институт машиноведения им. А. А. Благонравова РАН, Москва, Россия*

[2]*Московский государственный технический университет им. Н. Э. Баумана, Москва, Россия*

**e-mail: aproximandra@mail.ru*

***e-mail: vfil10@mail.ru*

Поступила в редакцию 24.11.2023 г.
После доработки 24.03.2024 г.
Принята к публикации 19.04.2024 г.

В статье изложены задачи прогнозирования возможного сценария непреднамеренных деструктивных воздействий (массовые воздействия – перепады напряжений, индустриальные электромагнитные помехи, воздействия природного характера) на распределенную автоматизированную систему управления. Предложены аналитические соотношения для оценки последствий подобных деструктивных воздействий (система передачи сигналов, система связи). Рассмотрен один из возможных сценариев таких воздействий на систему с учетом распределения их интенсивности.

Ключевые слова: устойчивость, автоматизированная система управления, непреднамеренные воздействия, динамический процесс, показатели комплексной устойчивости, контрвоздействия системы, прогнозирование, стабилизация

DOI: 10.31857/S0235711924040111, **EDN:** OYLEDL

Обобщенную оценку комплексной устойчивости (КУ) автоматизированной системы управления (АСУ) можно характеризовать значениями наиболее важных ее параметров, которые в совокупности будут в целом определять качество функционирования системы. При этом, с учетом прогнозирования некоторых непреднамеренных (случайных) воздействий, представляющих собой динамический процесс, показатель КУ будет непрерывно изменяться в соответствии со степенью и характером этих воздействий на узлы системы.

Оценивание качества КУ АСУ осуществляется с целью определения необходимых управляющих (корректирующих функционирование системы) контрвоздействий внутри системы, определения требуемых ресурсов для восстановления вышедших из строя элементов (узлов) системы, а также подготовке мероприятий и настройки параметров АСУ для стабилизации КУ [1, 9].

При получении оценки изменения КУ после непреднамеренных воздействий решаются задачи уточнения прогнозирования состояния АСУ с целью повышения КУ до требуемого уровня (это комплексная устойчивость, она же КУ), а также проводится разработка методики такого прогнозирования, которая, в свою очередь, должна

удовлетворять требованиям по определению границ неустойчивого состояния АСУ [2–5]. В статье рассматривается определение исходных данных для прогнозирования в соответствии с методикой и учитываются управляющие воздействия, необходимые КУ системы. Эти управляющие воздействия могут формироваться как внутри, так и снаружи системы на основе учета результатов прогнозирования непреднамеренных деструктивных воздействий.

При получении оценки комплексной устойчивости с учетом прогнозирования непреднамеренных воздействий решаются следующие задачи: 1) уточнение цели и постановки задачи прогнозирования; 2) разработка методики прогнозирования, обеспечивающей определение возможного снижения КУ АСУ после воздействий; 3) определение исходных данных для прогнозирования в соответствии с разработанной методикой; 4) установление сроков проведения расчетов и оформления результатов прогнозирования; 5) определение перечня мероприятий по повышению КУ АСУ, учитывающих результаты прогнозирования.

Поставленные задачи позволяют осуществить общую (вербальную) постановку задачи прогнозирования и определить исходные данные для нее.

Заданы: 1. Границы интервалов непреднамеренных воздействий на распределенную АСУ (предельное число воздействий). **2.** Возможности по снижению ущерба от непреднамеренных воздействий (вероятности выбора оптимальных по устойчивости системы параметров, вероятности успешной физической защиты системы) [1, 15].

Процесс решения задачи включает следующие основные этапы: 1. Определение возможного сценария непреднамеренных воздействий с учетом заданных ограничений возможностей. **2.** Расчет вероятностей выхода из строя элементов системы с учетом выбранного сценария непреднамеренных воздействий. **3.** Распределение ресурса воздействий на систему. **4.** Расчет условных вероятностей степеней выхода из строя элементов системы. **5.** Постановку задачи для повышения устойчивости конкретного элемента системы. **6.** Разработку алгоритма решения поставленной задачи.

Прогнозирование возможного сценария. Определение возможностей непреднамеренных воздействий осуществляется в соответствии с разработанным сценарием воздействий, который периодически корректируется с учетом текущей ситуации.

Сценарий необходим для определения (моделирования) количества, вида и моментов непреднамеренных воздействий на систему [6–9]. Один из возможных вариантов сценария воздействий на АСУ имеет вид, представленный на рис. 1.

В моменты $t_k^{\text{г}}$, $k = \overline{1,m}$, проводится моделирование нескольких групповых воздействий (ГВ) на систему, интенсивность которых распределена по закону Вейбулла, а в моменты t_k°, $k = \overline{1,n}$ – одиночные воздействия, проходящиев течение времени $T_{\text{о}}$, начиная с момента $t_{\text{о}}$ и завершая моментом $t_{\text{з}} = t_{\text{о}} + T_{\text{о}}$, где m и n – заданные числа групповых и одиночных воздействий (ОВ) соответственно.

Случайные моменты $t_k^{\text{г}}$ групповых воздействий равномерно распределены на соответствующих заданных соприкасающихся интервалах времени $I_k^{\text{г}} = (t_{k-1}, t_k)$ длиной $T_k = t_k - t_{k-1}$, т.е. на каждом из этих k-х интервалов ожидается одно k-е групповое воздействие в момент $t_k^{\text{г}}$. Определены минимально допустимые промежутки времени ΔT между соседними массовыми непреднамеренными воздействиями [16, 17], $\Delta T \le t_k^{\text{г}} - t_{k-1}^{\text{г}}$, и продолжительность каждого группового воздействия Δt. Случайные моменты времени одиночных воздействий t_k° равномерно распределены на одном заданном интервале $I^{\text{о}} = (t_{\text{н}}, t_{\text{з}})$ длиной $T_{\text{о}} = t_{\text{з}} - t_{\text{н}}$, где $t_{\text{н}}$ – начальное время интервала, $t_{\text{з}}$ – завершающее время интервала.

В результате этого процесса, при имитационном моделировании, моменты массовых и одиночных воздействий будут определяться с помощью следующих выражений [5, 6]:

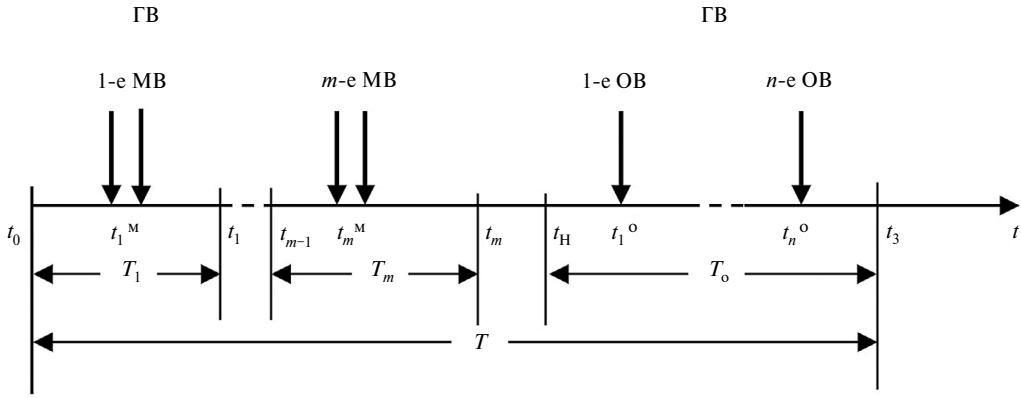

Рис. 1. Схема обобщенного сценария непреднамеренных групповых и одиночных воздействий на распределенную АСУ.

$$t_k^{\text{г}} = t_0 + T_k x_k + \sum_{j=1}^{k-1} T_j, \text{ при } t_{k+1}^{\text{г}} - t_k^{\text{г}} \geq \Delta T,\ k = \overline{1,m}; \tag{1}$$

$$t_k^0 = t + T_0 x_k^0,\ k = \overline{1,n}, \tag{2}$$

где x_k – равномерно распределенное случайное число, генерируемое датчиком случайных чисел $R(0, \underline{1}), x_k \in (0, 1)$. При этом генерация каждого следующего случайного числа $x_k,\ k = \overline{1,m}$, продолжается до тех пор, пока не будет выполнено условие $t_k{}^{\text{г}} - t_{k-1}{}^{\text{г}} \geq \Delta T$. Полученные значения $t_k{}^{\text{о}}$ можно затем ранжировать по возрастанию.

Пример. Будем использовать для расчетов следующие исходные данные: $t_0 = 0$; $m = 2$; $n = 3$; $T_1 = T_2 = 1$; $\Delta T = 0.5$; $T_{\text{о}} = 2$; $t_{\text{н}} = 2$.

Необходимо определить случайные моменты времени $t_1{}^{\text{г}}$; $t_2{}^{\text{г}}$; $t_1{}^{\circ}$; $t_2{}^{\circ}$, $t_3{}^{\circ}$ групповых и одиночных деструктивных воздействий.

По формуле (1) получаем

$$t_1 = t_0 + T_1 x_1 = 0 + 1 \cdot 0.4 = 0.4;$$

$$t_2 = t_0 + 1 + T_2 x_2 = 0 + 1 + 1 \cdot 0.8 = 1.8.$$

Так как $t_2{}^{\text{г}} - t_1{}^{\text{г}} = 1.8 - 0.4 = 1.4 > \Delta T = 0.5$, то $t_1{}^{\text{г}} = 0.4$; $t_2{}^{\text{г}} = 1.8$.

По формуле (2) получаем

$$t_1{}^{\text{о}} = t + T_{\text{о}} x_1 = 2 + 2 \cdot 0.7 = 3.4;$$

$$t_2{}^{\text{о}} = t + T_{\text{о}} x_1 = 2 + 2 \cdot 0.1 = 2.2;$$

$$t_1{}^{\text{о}} = t + T_{\text{о}} x_1 = 2 + 2 \cdot 0.4 = 2.8.$$

Ранжируем полученные значения по возрастанию: $t_1{}^{\text{о}} = 2.2$; $t_2{}^{\text{о}} = 2.8$; $t_3{}^{\text{о}} = 3.4$.

В зависимости от значений T можно применять следующие группы сценариев: 1) $T \geq 180$ суток; 2) $30 \leq T < 180$ суток; 3) $T < 30$ суток и др.

Возможны и другие более неблагоприятные сценарии [9–13]. Таким образом, при моделировании непреднамеренных деструктивных воздействий на АСУ в соответствии со сценарием нужно использовать следующие значения интервалов времени из общей схемы сценария, выраженные в часах: $T = 120$; $I_1^{\text{г}} = (0, 24]$; $I_2^{\text{г}} = (24, 48]$; $I_3^{\text{г}} = (48, 72]$; $t_{\text{о}} = 0$; $T_1 = T_2 = T_3 = 24$; $\Delta T = 6$; $I^{\circ} = (72, 120]$; $t_{\text{н}} = 72$; $t_{\text{з}} = 120$; $T_{\text{о}} = 48$. При этом число групповых непреднамеренных воздействий $m = 3$, а число одиночных воздействий n будет определяться исходя из требуемого времени снижения КУ.

Подставляя полученные значения в формулы (1) и (2), получим выражения для определения моментов воздействий (при $t_{\text{о}} = 0$)

$$t_k^{\text{м}} = 24x_k + (k-1)24,\ t_{k+1}^{\text{м}} - t_k^{\text{м}} \geq 6,\ k = 1, 2, 3;$$

$$t_k^0 = 72 + 48x_k,\ k = \overline{1,n}.$$

При определении вероятности эффективного непреднамеренного воздействия будем предполагать, что для достижения результата по снижению КУ АСУ будет производиться R воздействий [1, 14, 21]. В результате этого вероятность снижения КУ АСУ будет определяться, с помощью формулы [5, 6]:

$$P_A = 1 - (1 - P_C)^R,$$

где P_C – вероятность снижения устойчивости при единичном воздействии.

Вероятность P_C можно определить с помощью соотношения [5, 6]

$$P_C = P_1P_2P_3P_4P_5,$$

где P_1 – вероятность правильного выбора управляющих воздействия из всех возможных вариантов; P_2 – вероятность "эффективного" воздействия; P_3 – вероятность несрабатывания, как и в любой АСУ, системы защиты или оператора АСУ; P_4 – вероятность эффективного поиска уязвимости в АСУ подсистемой защиты или оператором; P_5 – условная вероятность "эффективного" воздействия после выполнения поиска уязвимости АСУ.

Значения данных вероятностей зависят от типа распределенной АСУ и возможностей воздействующих факторов.

При определении вероятностей "эффективного" воздействия необходимо иметь сведения об арсенале возможных воздействий на АСУ в соответствии с выбранным сценарием. Для получения подобных сведений необходимо решить ряд распределительных задач, учитывающих специфику воздействий, число, и эффективность подсистем защиты распределенной АСУ, структуру АСУ, важность и степень влияния состояния ее элементов на КУ в целом [16–18]. Результатом решения задачи прогнозирования непреднамеренных воздействий в распределении восстановительных ресурсов (очередность, средства, интенсивность) могут быть значения различных коэффициентов, характеризующих воздействия, таких как коэффициент группового воздействия

$$\alpha_{jk} = N_{jk}/N_j,$$

где N_{jk} – число объектов АСУ j-го типа, на которые нацелены деструктивные воздействия, производимые на k-ом шаге моделирования; N_j – общее число объектов АСУ j-го типа.

В табл. 1 приведен вариант распределения непреднамеренных воздействий с помощью коэффициентов между объектами АСУ при условии трех групповых воздействий.

Таблица 1. Коэффициенты групповых воздействий

Узлы АСУ	α_{j1} ($k = 1$)	α_{j2} ($k = 2$)	α_{j3} ($k = 3$)
3, 4	0.5	0.3	0.2
6	0.6	0.3	0.1
5, 7	0.6	0.3	0.1

Таблица 2. Границы степеней выхода из строя АСУ

s	Наименование степени	Нижняя граница H_s	Верхняя граница B_s	Интервальная оценка P_{ys} степени s	Точечная оценка P_{ys} степени s
1	Слабая	0	0.1	0.25–0.35	0.3
2	Средняя	0.1	0.2	0.35–0.45	0.4
3	Сильная	0.2	0.4	0.1–0.2	0.1
4	Полная	0.4	1.0	0.15–0.3	0.2

Эффективность деструктивных воздействий на АСУ зависит от их интенсивности и надежности ее подсистемы защиты. При этом степень успешного воздействия оценивается с помощью критерия [9]

$$H_s < n_э/N_э \le B_s,$$

где H_s, B_s – нижняя и верхняя границы относительного числа деструктивных воздействий при s-й степени их эффективности; $n_э$ – число деструктивных воздействий; $N_э$ – общее число возможных воздействий.

Степени эффективности деструктивных воздействий разумно разделить на четыре степени: слабая (отсутствие ощутимого влияния на работоспособность), средняя (сохранение работоспособности основных подсистем), сильная (вывод из строя с возможностью быстрого восстановления) и полная (вывод из строя), границы которых H_s, B_s определяются на основе экспертного опроса с учетом возможностей возврата к работоспособному состоянию [2, 18–21].

В табл. 2 приведен вариант предполагаемых границ степеней воздействий, интервальных и точечных оценок условных вероятностей этих степеней.

Условная вероятность P_{ys} степени воздействия s при условии вывода из строя АСУ определяется на основании статистических данных о результатах воздействий. При этом точечная оценка условной вероятности равна $P_{ys} = N_{пs}/N_п$, где $N_{пs}$ – число выведенных из строя узлов АСУ; $N_п$ – общее число выведенных из строя узлов АСУ.

Интервальная оценка величины P_{ys} при заданной доверительной вероятности проводится с помощью метода Монте-Карло [19, 21].

Вывод. В зависимости от прогнозируемого сценария воздействий на распределенную АСУ, учитывающего последовательные групповые и одиночные деструктивные воздействия, конечным итогом расчетов можно рассматривать интервалы s, поскольку их значения дают возможность определить требуемые ресурсы для восстановления КУ системы. В свою очередь каждому из полученных интервалов соответствуют значения оценок интервальной и точечной условных вероятностей P_{ys}.

Финансирование. Данная работа финансировалась за счет средств бюджета Институт машиноведения им. А.А. Благонравова РАН и Московский государственный

технический университет им. Н. Э. Баумана. Никаких дополнительных грантов на проведение или руководство данным конкретным исследованием получено не было.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. *Vasil'ev Yu. S., Zegzhda D. P., Poltavtseva M. A.* Problems of security in digital production and its resistance to cyber threats // Autom. Control Comput. Sci. 2018. V. 52 (8). P. 1090.
2. *Kotenko I. V., Saenko I. B.* The architecture of the system of intelligent information protection services in critical infrastructures // Tr. S.-Peterb. Inst. Inf. Avtom. Ross. Akad. 2013. No. 1. P. 21.
3. *Konoplev A. S., Kalinin M. O.* Tasks of providing information security in distributed computing networks // Aut. Control Comp. Sci. 2016. V. 50. P. 669.
4. *Kakubava R., Khurodze R.* Technical systems with structural and time redundancy: a probabilistic analysis of their performance // Autom. Remote Contr. 2004. V. 65. P. 825.
5. *Korolyuk V. S., Limnios N.* Stochastic Systems and Merging Phase. Singapore: Imperial College Press, 2005.
6. *Korolyuk V. S., Korolyuk V. V.* Stochastic Models of Systems. Dordrecht: Kluwer, 1999.
7. *Zegzhda D. P., Vasil'ev Y. S., Poltavtseva M. A.* Approaches to Modeling the Security of Cyberphysical Systems // Aut. Control Comp. Sci. 2018. V. 52. P. 1000.
8. *Dakhnovich A. D., Moskvin D. A., Zegzhda D. P.* Analysis of the Information Security Threats in the Digital Production Networks // Aut. Control Comp. Sci. 2018. V. 52. P. 1071.
9. *Osadchy S. I., Zozulya V. A., Ladanyuk A. P.* Optimal Robust Control of a Robots Group // Aut. Control Comp. Sci. 2019. V. 53. P. 298.
10. *Boegra O. H., Kwakernaak H., Meinsma G.* Design Methods for Control Systems // Notes of Course Dutch Institute of Systems and Control, 2006.
11. *Sharifov Y. A.* Necessary Optimality Conditions of First and Second Order for Systems with Boundary Conditions // Trans. Nat. Acad. Sci. Azerbaijan. Ser. Phys.-Techn. Math. Sci. 2009. V. 28 (1). P. 189.
12. *Tomasi W.* Electronic Communication Systems: Fundamental through Advanced. Pearson Education. N.J.: Upper Saddle River, 2004. 1163 p.
13. *Proakis J. G., Salehi M.* Digital communications. 5th ed. New York: McGraw-Hill, 2008. 1170 p.
14. *Kwakernaak H., Sivan R.* Linear Optimal Control Systems. New York: Wiley, 1972; Moscow: Mir, 1977.
15. *Chervyakov N. I., Kalmykov I. A., Shelkunova Yu. O., Beregnoy V. V.* Mathematical model of a neural network for error correction in a non-positional code of extended Galua field // Neurocomput.: Dev. Appl. 2003. No. 8–9. P. 10.
16. *Aldairi A., Tawalbeh L.* Cyber security attacks on smart cities and associated mobile technologies // Procedia Comput. Sci. 2017. V. 109. P. 1086.
17. *Shannon C. E.* A Mathematic Theory of Communications // Reprinted with corrections from Bell Syst. Tech. J. 1948. V. 27 (7, 10). P. 379, 623.
18. *Kalpana P.* Cloud Computing // Manfred Milchrahm. 2013. V. 3 (1). P. 47.
19. *Bhattacharyya D. K., Kalita J. K.* Network Anomaly Detection. A Machine Learning Perspective. CRC Press, 2013. 366 p.
20. *Skrobanek P.* Intrusion Detection Systems. Intech, 2011. 113 p.
21. *Maksimov M. V., Bobnev M. P., Krivitskiy B. Kh.* Protection against radio interference. M.: Sov. radio, 1976.