

<https://doi.org/10.18322/PVB.2019.28.02.47-56>

УДК 681.518.5

Формализованная модель оценки надежности функционирования тепловых электрических станций

© **Е. В. Гвоздев**^{1(✉)}, **С. Ю. Бутузов**², **Т. Г. Сулима**¹, **С. Б. Арифджанов**³

¹ Академия гражданской защиты МЧС России (Россия, 141435, Московская обл., г. Химки, мкр. Новогорск)

² Академия ГПС МЧС России (Россия, 129366, г. Москва, ул. Бориса Галушкина, 4)

³ Кокшетауский технический институт Комитета по чрезвычайным ситуациям МВД Республики Казахстан (Республика Казахстан, 020000, Акмолинская обл., г. Кокшетау, ул. Акана-серы, 136)

РЕЗЮМЕ

Введение. В отраслевой структуре управления России важное место занимают территориально распределенные объекты (филиалы) крупных производственных предприятий топливно-энергетического комплекса (ТЭК). Рассматриваемые предприятия в соответствии с утвержденными законодательством критериями относятся к категории опасных производственных объектов. Важной задачей является определение причины возникновения опасности.

Методы исследования. Для обнаружения опасностей в любых автоматизированных системах управления используются методы, с помощью которых осуществляется сбор информации о параметрических значениях функционирования производственных объектов. Для проведения исследований по обнаружению опасностей применяется ряд подходов, основанных: на определении параметров (инвариантов) моделей контролируемых объектов; на решении задач моделирования (прогнозировании); на использовании аналитической избыточности. Существует безмодельный метод обнаружения опасностей в автоматизированных системах управления, в основе которого заложено представление только данных сигналов управления и измерений параметров функционирования динамических объектов. Он основан на алгебраическом условии разрешимости задачи идентификации математической модели функционирования динамического объекта.

Постановка задачи. Требуется на основе результатов измерений входных сигналов, поступающих в автоматизированную систему управления, разработать параметрические значения для критической зоны возникновения опасностей в целях отображения информации на дисплее автоматизированного рабочего места оператора.

Решение задачи. Предложено представлять модели объекта в исправном и неисправном состояниях в виде матриц, что позволит решать задачи идентификации замкнутых объектов для любых входных сигналов, независимо от наличия информации о параметрах системы управления. Быстродействие и точность обнаружения факта и времени возникновения опасности (отказа системы) определяются частотой дискретизации сигналов и совпадают с интервалом времени между двумя последовательными измерениями.

Заключение. Достоинством предлагаемого подхода является его независимость от параметров модели контролируемого объекта. Использование предлагаемого подхода для обнаружения дает возможность перевести систему управления безопасностью предприятия на новый качественный уровень за счет постоянной отслеживаемости процесса функционирования объектов производства, повышения скорости и достоверности обнаружения факта и времени возникновения опасности.

Ключевые слова: система управления безопасностью ТЭС; математическая модель; оценка надежности ТЭС; распределенные каналы передачи информации, опасные факторы ТЭС.

Для цитирования: Гвоздев Е. В., Бутузов С. Ю., Сулима Т. Г., Арифджанов С. Б. Формализованная модель оценки надежности функционирования тепловых электрических станций // Пожаровзрывобезопасность/ Fire and Explosion Safety. — 2019. — Т. 28, № 2. — С. 47–56. DOI: 10.18322/PVB.2019.28.02.47-56.

✉ Гвоздев Евгений Владимирович, e-mail: evgvozdev@mail.ru

Formal model of evaluating the reliability of thermal power plants

© **E. V. Gvozdev**^{1(✉)}, **S. Yu. Butuzov**², **T. G. Sulima**¹, **S. B. Arifjanov**³

¹ Civil Defence Academy of Emercom of Russia (md. Novogorsk, Khimki, Moscow Region, 141435, Russian Federation)

² State Fire Academy of Emercom of Russia (Borisa Galushkina St., 4, Moscow, 129366, Russian Federation)

³ Kokshetau Technical Institute of the Committee for Emergency Situations of the Ministry of Internal Affairs of the Republic of Kazakhstan (Akan-seri St., 136, Akmol Region, Kokshetau, 020000, Republic of Kazakhstan)

ABSTRACT

Introduction. In the branch structure of management of Russia an important place is occupied by geographically distributed objects (branches) of large industrial enterprises of the fuel and energy complex. The considered enter-

prises, in accordance with the criteria approved by the legislation, belong to the category of hazardous production facilities. An important task is to determine the cause of the danger.

Methods of research. To detect hazards in any automated control systems used methods by which information is collected on the parametric values of the functioning of production facilities. To conduct research on the detection of hazards, a number of approaches are used: based to determine the parameters (invariants) of the models of controlled objects; to solve the problems of modeling (forecasting); to use analytical redundancy. There is a model-free method of hazard detection in automated control systems, which is based on the representation of only the data of control signals and measurements of the parameters of the functioning of dynamic objects. It is based on the algebraic condition of solvability of the problem of identification of a mathematical model of dynamic object functioning.

Problem statement. It's required on the basis of the measurement results the input signals coming into the automated control system, to develop a parametric value for the critical zone of occurrence of hazards with the aim of displaying information on the display of the workstation operator.

Problem solution. It is offered to represent models of object, in serviceable and faulty States, in the form of matrices that will allow solving problems of identification of the closed objects for any input signals, irrespective of availability of information on parameters of control system. The speed and accuracy of detection of the fact and time of danger (system failure) are determined by the sampling frequency of the signals and coincide with the time interval between the two consecutive measurements.

Conclusion. The advantage of the proposed approach is its independence from the parameters of the controlled object model. The use of the proposed approach for detection makes it possible to transfer the security management system of the enterprise to a new qualitative level due to constant traceability of the process of functioning of production facilities, increasing the speed and reliability of detection of the fact and time of danger.

Keywords: safety management system of TPP; mathematical model; reliability evaluation TPP; distributed communication channels; hazards TPP.

For citation: E. V. Gvozdev, S. Yu. Butuzov, T. G. Sulima, S. B. Arifjanov. Formal model of evaluating the reliability of thermal power plants. *Pozharovzryvobezopasnost/Fire and Explosion Safety*, 2019, vol. 28, no. 2, pp. 47–56 (in Russian). DOI: 10.18322/PVB.2019.28.02.47-56.

✉ Evgeniy Vladimirovich Gvozdev, e-mail: evgvozdev@mail.ru

Введение

В отраслевой структуре управления России важное место занимают территориально распределенные объекты (филиалы) крупных производственных предприятий топливно-энергетического комплекса (ТЭК). К основным организациям ТЭК, осуществляющим производство, передачу, распределение тепловой и электрической энергии, относятся тепловые электрические станции (ТЭС), которые не только производят электроэнергию, но и являются источниками тепловой энергии в централизованных системах теплоснабжения. Рассматриваемые предприятия в соответствии с критериями, прописанными в Федеральном законе № 123-ФЗ (далее — ФЗ № 123), относятся к категории опасных производственных объектов (далее — ОПО). Признаками опасности ОПО являются:

- использование в производственной деятельности аварийно-химических отравляющих веществ (АХОВ);
- аккумулярование и возможный несанкционированный выброс огромных запасов кинетической, тепловой, акустической и вибрационной энергии из-за высокого давления в трубопроводах подачи пара и горячей воды;
- использование водорода для охлаждения обмотки и возбуждения турбин;
- хранение значительных запасов мазута для использования в качестве топлива в аварийных ситуациях.

В проведенных исследованиях [1–4] автор предлагает рассматривать безопасность предприятий ТЭК в комплексе, в виде совокупности взаимодействующих функциональных направлений безопасности (промышленной и пожарной безопасности, предупреждения и ликвидации ЧС природного и техногенного характера, охраны труда и экологической безопасности, антитеррористической защищенности и т. д.), т. е. представлять ее в виде системы комплексной техносферной безопасности (СКТБ) предприятия для реализации главной цели, направленной на минимизацию (исключение условий) вероятности возникновения опасностей (рис. 1).

Безопасность предприятия ТЭК определяется способностью его территориально распределенных объектов (филиалов) противостоять реализации деструктивных воздействий, не допускать катастрофических разрушений на этапах закритического функционирования объектов защиты после достижения предельных состояний. К источникам закритического функционирования относятся:

- естественная вариативность параметров объекта и внешней среды, ограниченность знаний о событиях и процессах, протекающих в сложных технических системах объекта;
- неточность имеющихся статистических данных и оценок;
- несовершенство используемого контрольно-измерительного оборудования и математических моделей [5–7].



Рис. 1. Отраслевые направления безопасности в составе СКТБ предприятия

Fig. 1. Industry security areas incoming the content of the enterprise SKTB

Вопросы обеспечения безопасной эксплуатации ОПО являются приоритетными для государства. В связи с этим разрабатываются и принимаются к исполнению основы единой государственной политики для отраслевых направлений безопасности на долгосрочный период, утверждаемые Указами Президента России. Например, в документе стратегического планирования “Основы государственной политики в области защиты населения и территорий от чрезвычайных ситуаций на период до 2030 года”, утвержденном в январе 2018 г. Указом Президента России, определена главная цель по реализации рассматриваемого направления — *обеспечение устойчивого социально-экономического развития РФ, а также приемлемого уровня безопасности жизнедеятельности населения в чрезвычайных ситуациях (ЧС)*.

Приемлемый уровень безопасности жизнедеятельности населения в ЧС будет поддерживаться за счет требуемого уровня защищенности в подсистемах безопасности (см. рис. 1), создания в них запаса надежности для устойчивого функционирования.

Производственные предприятия ТЭС имеют множество площадок (территорий) ОПО, поскольку их производственная деятельность связана с транспортировкой и хранением углеводородов, обращением в технологическом процессе АХОВ, аккумулированием и возможным несанкционированным выбросом огромных запасов кинетической, тепловой, акустической и вибрационной энергии, получаемой при переработке углеводородов технологическим оборудованием.

К технологическому оборудованию ТЭС относятся:

- трубопроводы, работающие под давлением, для подачи углеводородов;

- динамическое оборудование (насосы, компрессоры, турбины);
- статическое оборудование (высоконагруженные сосуды, в том числе колонны, сепараторы, адсорберы, технологические трубопроводы, работающие при криогенных и высоких температурах) [8–10].

Для надежной реализации контроля и регулирования режимов работы технологического оборудования ТЭС используются специальные автоматизированные системы управления технологическим процессом (АСУ ТП), обеспечивающие надежный уровень их функционирования в течение всего срока эксплуатации ТЭС. С этой же целью принимаются меры по минимизации:

- отказов в аппаратуре;
- воздействия отказов на выполнение функций управления и контроля;
- времени на восстановление аппаратуры [8, 11–13].

Реализация указанных требований обеспечивается за счет надежного исполнения функций контроля и управления в АСУ ТП, в которые входит индивидуальная защита АСУ ТП и возможность отключения всех ее каналов ввода/вывода, а также контроль состояний автоматов защиты контроллерной части и запорно-регулирующей арматуры [14, 15].

Отказы, возникающие в процессе функционирования подсистем обеспечения ТЭС, являются наиболее опасными и могут привести к чрезвычайной ситуации. При возникновении таких отказов изменяются показатели функциональных параметрических значений обеспечивающих подсистем, моментные характеристики подсистем управления, структура системных связей [11, 14, 16, 17].

В сложившихся условиях функционирования объектов ТЭС возникает необходимость, наряду с реализуемыми методами обеспечения безопасности их технологического процесса, дополнительно использовать наиболее прогрессивные методы, апробированные на моделях других динамических объектов, для решения важных задач по своевременному выявлению (до наступления аварийной ситуации) предпосылок к деструктивному воздействию на персонал, оборудование и имущество ТЭС, т. е. своевременному определению места и причины возникновения отказа [18–20].

Методы исследования

Для обнаружения отказов в любых автоматизированных системах управления (АСУ), как правило, используются методы [16, 21], предусматривающие наличие априорной информации о параметрических значениях функционирования производственных объектов, которые в некоторых случаях по-

лучить бывает достаточно трудно, а иногда принципиально невозможно.

С точки зрения принципов обнаружения отказов выделяется ряд подходов, основанных:

- *первый*, наиболее применяемый в АСУ, — на определении параметров (инвариантов) моделей контролируемых объектов [9, 21];
- *второй* — на решении задач моделирования (прогнозирования) [16, 18];
- *третий* — на использовании аналитической избыточности [6, 19].

Первый принцип требует знания инвариантов объекта диагностирования. Его суть сводится к выявлению некоторых характеристик объекта, остающихся неизменными при его нормальном функционировании и изменяющихся при возникновении отказов. Далее эти характеристики используются в качестве прямых или косвенных диагностических признаков. Они могут быть двух типов — параметрические и сигнальные (алгебраические). Основная трудность при контроле по параметрическим инвариантам связана со сложностью измерения реальных значений параметров, тогда как их номинальные значения бывают известны. При контроле по сигнальным инвариантам главная проблема состоит в необходимости непрерывного определения теоретических значений выходных сигналов, исходя из известных текущих значений входных сигналов.

Второй принцип контроля опирается на использование моделей проверяемого объекта. Известны два главных подхода к решению задач обнаружения отказа такими методами — в пространстве сигналов и в пространстве параметров. Обнаружение отказов модельными методами в пространстве сигналов осуществляется путем генерации так называемой невязки и последующего анализа ее статистических свойств. В качестве генераторов невязки используются диагностические наблюдатели и диагностические устройства, основанные на соотношении паритета. Во втором подходе определяются оценки текущих значений физических параметров объекта, которые сравниваются с номинальными. Подход может быть реализован с использованием методов параметрической идентификации. Однако применение данных методов существенно ограничивается проблемой неидентифицируемости объектов управления с замкнутой обратной связью [22].

Третий принцип контроля связан с использованием аналитической избыточности. Согласно этому принципу обнаружение отказов осуществляется на основе проверки аналитических зависимостей, существующих между измеряемыми входами и выходами системы. Такие зависимости (их называют контрольными условиями или уравнениями) могут связывать сигналы, относящиеся к одному и тому же

моменту времени, и тогда говорят об алгебраических инвариантах, либо к разным моментам, и тогда говорят о динамических инвариантах или временной избыточности. В схемах аналитической избыточности результирующее различие формируется из проверки на непротиворечивость различных переменных, называемых рассогласованиями. Рассогласование должно быть равно нулю, когда система работает нормально, и отличаться от нуля в случае отказа. Это свойство рассогласования используется для определения того, есть отказ в системе или нет.

Применение методов, основанных на моделях, неизбежно приводит к увеличению пороговых значений используемых критериев при наличии ошибок в параметрах моделей. Это, в свою очередь, обуславливает увеличение времени обнаружения отказов и снижение достоверности определения времени их возникновения. При этом в некоторых случаях достоверное определение времени возникновения отказов становится невозможным в принципе [22, 23].

Широко известные методы, не использующие априорную информацию о параметрах модели, требуют длительного обучения либо используют статистические вычисления, которые сами подвержены неизбежным ошибкам. Получение точных и достоверных решений с помощью таких алгоритмов требует большого объема данных. Кроме того, они характеризуются высокими вычислительными затратами и низкими показателями быстродействия. Эти факторы определяют высокую вероятность ложного срабатывания или пропуска отказов на практике. В условиях эксплуатации применение таких методов может потребовать время, превышающее критическое время реакции АСУ ТП, и подсистемы обеспечения ТЭС могут перейти в невосстанавливаемое состояние [24].

Известен безмодельный метод обнаружения отказов в системах управления, в основе которого заложено представление только данных сигналов управления и измерений параметров функционирования динамических объектов [9, 23]. Он не требует априорной информации о параметрах их функционирования, не использует статистических вычислений и основан на алгебраическом условии разрешимости задачи идентификации функционирования динамических объектов, что делает возможным его применение в отношении подсистем обеспечения ТЭС при действии возмущений.

В настоящей работе предлагается новый подход к обнаружению отказов в подсистемах обеспечения ТЭС, позволяющий использовать только данные измерений входных и выходных сигналов системы управления. Он, так же как и упомянутый выше безмодельный метод, не требует априорной информации о параметрах объекта, не предусматривает решения

задачи прогнозирования, не применяет статистических вычислений, а основан на алгебраическом условии разрешимости задачи идентификации математической модели функционирования динамического объекта.

Постановка задачи. Пусть модель исправного динамического объекта с замкнутой системой управления представлена в пространстве состояний в виде [23]:

$$x_{i+1} = Ax_i + B(u_i + u_o), \quad (1)$$

$$u_i = Kx_i + Gv_i, \quad (2)$$

где A, B, K, G — матрицы соответственно собственной динамики, эффективности управления, регулятора и предкомпенсатора;

x — вектор состояния объекта размерности n_x ;

u — сигнал на выходе АСУ ТП, совпадающий при отсутствии опасности (отказа системы) с вектором отклонения органа управления размерности n_u ;

v — вектор входных сигналов размерности n_v ;

u_o — вектор допустимых отклонений параметров, запрограммированных и отображаемых в АСУ ТП, соответствующих равновесному состоянию динамического объекта;

$i = 0, I - 1$ — дискретное время до возникновения опасности (отказа системы);

I — момент возникновения опасности (отказа системы).

Запишем модель (1) в виде:

$$x_{i+1} = Ax_i + Bu_i + m_o(u_i + u_o), \quad (3)$$

где m_o — вектор постоянных коэффициентов, обусловленных допустимыми отклонениями параметров, отображаемых в АСУ ТП; $m_o = Bu_o$;

u_i — вектор допустимых отклонений параметров, запрограммированных и отображаемых в АСУ ТП, за временной период t .

При возникновении опасности (отказа системы) в АСУ ТП модель объекта будет иметь вид:

$$x_{j+1}^f = Ax_j^f + Bu_j^f + m_o; \quad (4)$$

$$u_j = Kx_j^f + Gv_i, \quad (5)$$

где $j = 0, I + 1, \dots$ — дискретное время после возникновения опасности (отказа системы);

x_j^f — вектор состояния опасности (отказа системы), отображаемый в критической зоне отклонения параметров, запрограммированных в АСУ ТП, которые описываются выражением

$$x_j^f = Fu_j + (I - F)u_o^f, \quad (6)$$

F — матрица возникновения опасности (отказа системы) в условиях снижения эффективности управления безопасностью производственных

территориально распределенных объектов управления;

$$F = \text{diag}[f(1) \dots f(k) \dots f(n_u)]; \quad (7)$$

u_o^f — вектор возникновения опасности (отказа системы), отображаемый в критической зоне отклонения в АСУ ТП;

$$u_o^f = [u_o^f(1) \dots u_o^f(k) \dots u_o^f(n_u)]. \quad (8)$$

Подставим (6) в (4) и запишем модель объекта с неисправной системой управления u_j :

$$x_{j+1}^f = Ax_j^f + B_f u_j + m_o^f, \quad (9)$$

где B_f — матрица эффективности управления неисправного объекта; $B_f = BF$;

m_o^f — постоянный вектор, характеризующий совокупное отклонение параметров, запрограммированных в АСУ ТП и отображаемых в критической зоне; $m_o^f = B(I - F)u_o^f + m_o$.

Требуется на основе результатов измерений входных сигналов, поступающих в АСУ ТП, разработать параметрические значения для критической зоны возникновения опасностей (отказа системы) в целях отображения информации на дисплее АСУ ТП. Это позволит лицу, принимающему решение (далее — ЛПР), принять обоснованное решение для устранения причин возникновения опасности, скорректировать управляемое воздействие на объект управления, подвергающийся опасности (отказ системы).

Решение задачи. Предположим, что наблюдение за объектом ведется на протяжении некоторого времени. Тогда модели объекта в исправном (3) и неисправном (9) состояниях будут иметь матричный вид:

$$X_{i+1} = AX_i + BU_i = m_o e;$$

$$X_{j+1}^f = AX_j^f + B_f U_j + m_o^f e,$$

где $X_i = [x_i \dots x_{i+h}]$; $X_j^f = [x_j^f \dots x_{j+h}^f]$;

$$U_i = [u_i \dots u_{i+h}]; U_j = [u_j \dots u_{j+h}]; e = [1 \dots 1];$$

h, h^f — количество шагов наблюдения за объектом соответственно в исправном и неисправном состояниях.

При этом задачи идентификации параметров модели контролируемого объекта в каждом случае описываются линейными правосторонними матричными уравнениями относительно неизвестных A, B, m_o, B_f, m_o^f :

$$[ABm_o] \begin{bmatrix} X_i \\ U_i \\ e \end{bmatrix} = X_{i+1}; \quad [AB_f m_o^f] \begin{bmatrix} X_j^f \\ U_j \\ e \end{bmatrix} = X_{j+1}^f. \quad (10)$$

Для решения матричных уравнений (10) воспользуемся результатами работы [14], где показано, что линейное матричное уравнение вида

$$XC = D$$

с известными матрицами C и D разрешимо относительно X тогда и только тогда, когда выполняется условие разрешимости

$$D\bar{C}^R = 0. \quad (11)$$

При этом все множество решений определяется формулой

$$X = [D\bar{C}^R \Theta] \begin{bmatrix} \bar{C}^L \\ \bar{C}^L \end{bmatrix} = D\bar{C} + \Theta\bar{C}^L, \quad (12)$$

где Θ — произвольная матрица;

\bar{C}^L, \bar{C}^R — левый и правый делители нуля максимального ранга (т. е. матрицы, для которых выполняются условия $\bar{C}^L C = 0, \bar{C}^R C = 0$);

\bar{C}^L, \bar{C}^R — левый и правый делители единицы ($\bar{C}^L C \bar{C}^R = I$);

$\bar{C} = \bar{C}^R \bar{C}^L$ — обобщенно-обратная матрица, определяемая с помощью канонического разложения вида:

$$C = \begin{bmatrix} \bar{C}^L \\ \bar{C}^L \end{bmatrix}^{-1} \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} [\bar{C}^R \bar{C}^R]^{-1}. \quad (13)$$

Каноническое разложение (13) имеет в общем случае неединственный вид и фактически формализует прямые и обратные эквивалентные преобразования матрицы [25]. Использование канонического разложения позволяет получать в аналитическом виде множество решений, имеющих минимальный ранг.

Тогда в соответствии с (11) условиями разрешимости задач идентификации моделей (10), т. е. условиями наличия хотя бы одного решения, являются эквивалентные с точностью до обозначения переменных выражения:

$$X_{i+1} \begin{bmatrix} X_i \\ U_i \\ e \end{bmatrix}^R = 0; \quad X_{j+1}^f \begin{bmatrix} X_j^f \\ U_j^f \\ e \end{bmatrix}^R = 0. \quad (14)$$

При выполнении условий разрешимости (14) все идентифицированные модели согласно (12) могут быть записаны в виде множеств:

$$\begin{aligned} [ABm_o] &= X_{i+1} \begin{bmatrix} X_i \\ U_i \\ e \end{bmatrix} + \Psi \begin{bmatrix} X_i \\ U_i \\ e \end{bmatrix}^L; \\ [AB_f m_o^f] &= X_{j+1}^f \begin{bmatrix} X_j^f \\ U_j^f \\ e \end{bmatrix} + \Upsilon \begin{bmatrix} X_j^f \\ U_j^f \\ e \end{bmatrix}^L, \end{aligned} \quad (15)$$

где Ψ, Υ — произвольные матрицы.

В соответствии с (15) условиями идентифицируемости, т. е. условиями получения единственного решения, являются равенства нулю левых делителей нуля:

$$\begin{bmatrix} X_i \\ U_i \\ e \end{bmatrix}^L = 0; \quad \begin{bmatrix} X_j^f \\ U_j^f \\ e \end{bmatrix}^L = 0. \quad (16)$$

Для определения условий их существования подставим выражения для управлений (2), (5) в (16):

$$\begin{aligned} \begin{bmatrix} X_i \\ U_i \\ e \end{bmatrix} &= \begin{bmatrix} I & 0 & 0 \\ K & G & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_i \\ V_i \\ e \end{bmatrix}; \\ \begin{bmatrix} X_j^f \\ U_j^f \\ e \end{bmatrix} &= \begin{bmatrix} I & 0 & 0 \\ K & G & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_j^f \\ V_j^f \\ e \end{bmatrix}, \end{aligned}$$

где $V_i = [v_i \dots v_{i+h}]$; $V_j = [v_j \dots v_{j+h}^f]$.

Тогда условия идентифицируемости (16) примут вид делителей нуля произведений блочных матриц:

$$\begin{bmatrix} I & 0 & 0 \\ K & G & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_i \\ V_i \\ e \end{bmatrix}^L = 0; \quad \begin{bmatrix} I & 0 & 0 \\ K & G & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_j^f \\ V_j^f \\ e \end{bmatrix}^L = 0,$$

которые при наличии левого делителя нуля матрицы предкомпенсатора ($\bar{G}^L G = 0$) всегда могут быть записаны в виде:

$$\begin{aligned} [0\bar{G}^L 0] \begin{bmatrix} I & 0 & 0 \\ K & G & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_i \\ V_i \\ e \end{bmatrix} &= 0; \\ [0\bar{G}^L 0] \begin{bmatrix} I & 0 & 0 \\ K & G & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_j^f \\ V_j^f \\ e \end{bmatrix} &= 0. \end{aligned}$$

Матрица предкомпенсатора преобразует входные сигналы в сигналы, поступающие непосредственно в АСУ ТП. В научном источнике [23] показано, что в этом случае проблема получения единственного решения задачи идентификации замкнутых объектов будет характерна для любых входных сигналов независимо от наличия информации о параметрах системы управления. Этот факт показывает, что на практике параметрические методы идентификации используются либо с учетом априорной информации о модели объекта, либо с помощью подачи тестовых сигналов непосредственно на АСУ ТП (орган управления) [24, 25].

Проанализируем более подробно условия разрешимости без непосредственного решения задач идентификации. Выражения (14) показывают, что задача идентификации линейной модели объекта разрешима как до, так и после возникновения опасностей (отказа системы). Однако непосредственно в мо-

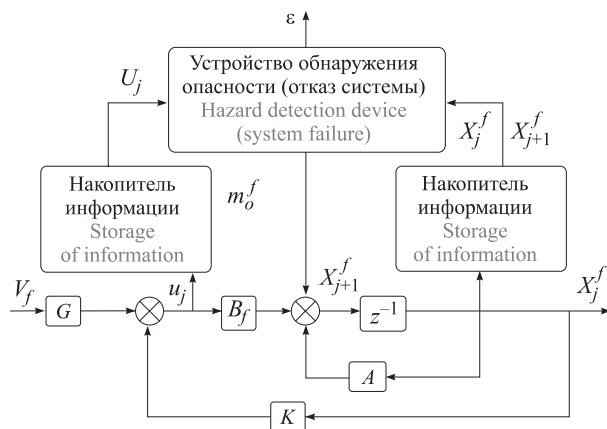


Рис. 2. Схема обнаружения опасности (отказа системы)

Fig. 2. The detection risk (system failure)

мент их возникновения поведение объекта не может быть описано с помощью единой линейной модели:

$$\begin{aligned} [X_{i+1} \ X_{j+1}^f] &= A [X_i \ X_j^f] + B[U_i \ U_j] + \\ &+ m_o[e \ e] + \Delta B_f[0 \ U_j] + \Delta m_o^f[0 \ e], \end{aligned}$$

где $\Delta B_f = B(F - I)$; $\Delta m_o^f = B(I - F)u_o^f$.

В связи с этим задача идентификации в этом случае не имеет точного решения, и условие разрешимости не выполняется:

$$\begin{aligned} [X_{i+1} \ X_{j+1}^f] \begin{bmatrix} X_i & X_j^f \\ U_i & U_j \\ e & e \end{bmatrix}^R &= \\ = [\Delta B_f \ \Delta m_o^f] \begin{bmatrix} 0 & U_j \\ 0 & e \end{bmatrix} \begin{bmatrix} X_i & X_j^f \\ U_i & U_j \\ e & e \end{bmatrix}^R &\neq 0. \end{aligned} \quad (17)$$

Этот факт позволяет использовать норму условия (17), характеризующую точность решения задачи идентификации [24]:

$$\varepsilon = \left\| [X_{i+1} \ X_{j+1}^f] \begin{bmatrix} X_i & X_j^f \\ U_i & U_j \\ e & e \end{bmatrix}^R \right\|, \quad (18)$$

где определяется ортогональный делитель нуля матрицы входных/выходных данных

$$\left(\begin{bmatrix} X_i & X_j^f \\ U_i & U_j \\ e & e \end{bmatrix}^R \right)^T \begin{bmatrix} X_i & X_j^f \\ U_i & U_j \\ e & e \end{bmatrix}^R = I$$

в качестве простого и эффективного критерия возникновения отказов в системе управления динамическим объектом (1).

На рис. 2 приведена схема работы алгоритма обнаружения опасности (отказа системы) согласно предложенному методу. Для формирования матриц входных/выходных данных в соответствии с требуемой шириной окна идентификации необходимо использовать накопители информации, данные из которых поступают в устройство обнаружения опасности (отказа системы), где реализован алгоритм вычисления нормы (18).

Для исправного объекта значение нормы (18) будет равно нулю или некоторому набору чисел, находящихся в секторе допустимых значений, и выйдет за пределы допустимых значений при обнаружении опасности (отказа системы).

Момент отклонения от допустимых значений, запрограммированных в АСУ ТП, совпадает с временем возникновения опасности (отказа системы) в данной системе поддержки управления. Таким образом, быстрдействие и точность обнаружения факта и времени возникновения опасности (отказа системы) определяются частотой дискретизации сигналов и совпадают с интервалом времени между двумя последовательными измерениями.

Заключение

В результате исследований разработан новый подход для обнаружения факта и времени возникновения опасности (отказа системы) в подсистемах функционирования ТЭС для формирования базы данных измерений сигналов, поступающих для обработки в АСУ ТП. Основным достоинством предлагаемого подхода является его независимость от параметров модели контролируемого объекта, что гарантирует факт передачи информации на АСУ ТП по обнаружению опасности (отказа системы) как до момента возникновения, так и после устранения выявленных отклонений от установленных системой показателей.

Использование предлагаемого подхода для обнаружения опасности (отказа системы) дает возможность перевести систему управления безопасностью предприятия на новый качественный уровень за счет постоянной отслеживаемости процесса функционирования объектов производства, повышения скорости и достоверности обнаружения факта и времени возникновения опасности (отказа системы).

СПИСОК ЛИТЕРАТУРЫ

1. Гвоздев Е. В. Разработка алгоритма отклонения от нормы для обнаружения опасности технической системой управления безопасностью на предприятии // XXI век. Техносферная безопасность. — 2018. — Т. 3, № 2(10). — С. 25–34. DOI: 10.21285/2500-1582-2018-2-25-34.

2. Гвоздев Е. В. Разработка метода обнаружения и агрегирования показателей опасностей, воздействующих на объекты защиты предприятия и окружающую среду // XXI век. Техносферная безопасность. — 2018. — Т. 3, № 3(11). — С. 69–81. DOI: 10.21285/1814-3520-2018-3-69-81.
3. Гвоздев Е. В. Анализ надежности функционирования системы комплексной техносферной безопасности предприятия на основе вероятностей деструктивного воздействия и его преодоления подсистемой безопасности // XXI век. Техносферная безопасность. — 2018. — Т. 3, № 4(12). — С. 51–66. DOI: 10.21285/1814-3520-2018-4-51-66.
4. Гвоздев Е. В. Обоснование централизованного управления комплексной безопасностью объектов защиты техносферы // XXI век. Техносферная безопасность. — 2017. — Т. 2, № 4(8). — С. 97–107.
5. Махутов Н. А., Пермяков В. Н., Ахметханов Р. С., Резников Д. О., Дубинин Е. Ф. Анализ рисков и обеспечение защищенности критически важных объектов нефтегазохимического комплекса : учеб. пособие. — Тюмень : ТюмГНГУ, 2013. — 560 с.
6. Sutton I. Process risk and reliability management. — 2nd ed. — Oxford : Gulf Professional Publishing, 2015. — 798 p. URL: <https://b-ok.org/book/2463300/b6cf53> (дата обращения: 01.12.2018).
7. Assessment of large power transformer risk mitigation strategies. — Fairfax : ICF, October 2016. URL: <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf> (дата обращения: 10.12.2018).
8. Махутов Н. А., Резников Д. О., Петров В. П., Кукова В. И. Нормативные подходы к обеспечению защищенности критически важных объектов // Безопасность в техносфере. — 2011. — № 4. — С. 5–12.
9. Billinton R., Allan R. N. Reliability assessment of large electric power systems. — Boston, MA : Springer, 1988. DOI: 10.1007/978-1-4613-1689-3.
10. Popoola J. J., Ponnle A. A., Ale T. O. Reliability worth assessment of electric power utility in Nigeria: Residential customer survey results. URL: http://www.journal.au.edu/au techno/2011/jan2011/journal143_article08.pdf (дата обращения: 10.12.2018).
11. Бутузов С. Ю., Любавский А. Ю. Оценка времени наработки на отказ накопителей информации автоматизированных систем пожаровзрывобезопасности // Технологии техносферной безопасности. — 2011. — Вып. 6(40). URL: https://elibrary.ru/download/elibrary_20329697_28243844.htm (дата обращения: 01.12.2018).
12. Aneiba A., Melad M. Performance evaluation of AODV, DSR, OLSR, and GRP MANET routing protocols using OPNET // International Journal of Future Computer and Communication. — 2016. — Vol. 5, No. 1. — P. 57–60. DOI: 10.18178/ijfcc.2016.5.1.444.
13. Bhavaraju M. P., Billinton R., Brown R. E., Endrenyi J., Li W., Meliopoulos A. P., Singh C. IEEE tutorial on electric delivery system reliability evaluation // IEEE Power Engineering Society (PES). — 2005. — Publication 05TP175. — P. 39–51.
14. Топольский Н. Г., Бутузов С. Ю., Минеев Е. Н. Автоматизированная система предотвращения аварийных режимов электродвигателей при обнаружении токов утечки и короткого замыкания // Технологии техносферной безопасности. — 2015. — Вып. 3(61). — С. 246–251. URL: https://elibrary.ru/download/elibrary_25101416_29886300.pdf (дата обращения: 01.12.2018).
15. Abhilash B. T., Manjunatha H. M., Ranjan N. A., Tejamoorthy M. E. Reliability assessment of induction motor drive using failure mode effects analysis // IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE). — 2013. — Vol. 6, Issue 6. — P. 32–36.
16. Billinton R., Li W. Reliability assessment of electric power systems using Monte Carlo methods. — New York — London : Plenum Press, 1994. — 351 p. DOI: 10.1007/978-1-4899-1346-3.
17. Special reliability assessment: potential bulk power system impacts due to severe disruptions on the natural gas system. Technical Report. — Atlanta : NERC, November 2017. URL: https://www.nerc.com/ra/RAPA/ra/Reliability%20Assessments%20DL/NERC_SPOD_11142017_Final.pdf (дата обращения: 10.12.2018).
18. Ястребенецкий М. А., Иванова Г. М. Надежность автоматизированных систем управления технологическими процессами : учеб. пособие для вузов. — М. : Энергоатомиздат, 1989. — 264 с.
19. Биргер И. А. Техническая диагностика. — М. : Машиностроение, 1978. — 240 с.
20. Арефьева Е. В., Рыбаков А. В., Арифджанов С. Б. Оценка техногенного риска на основе интегрального индекса // Новости науки Казахстана. — 2018. — Вып. 1(135). — С. 30–42.
21. Мироновский Л. А. Функциональное диагностирование динамических систем. — М.—СПб. : Изд-во МГУ-ГРИФ, 1998. — 256 с.
22. Зыбин Е. Ю. Об идентифицируемости линейных динамических систем в замкнутом контуре в режиме нормальной эксплуатации // Известия ЮФУ. Технические науки. — 2015. — № 4(165). — С. 160–170.

23. Зыбин Е. Ю., Косьянчук В. В. Алгебраический критерий обнаружения факта и времени возникновения отказов в системах управления динамическими объектами // Известия Российской Академии наук. Теория и системы управления. — 2016. — № 4. — С. 50–61. DOI: 10.7868/S0002338816040168.
24. Зыбин Е. Ю. Об особенности моделирования и идентификации дискретных систем в пространстве состояний // Управление в технических системах : матер. конф. — СПб. : ГНЦ РФ–ЦНИИ “Электроприбор”, 2010. — С. 23–26.
25. Зыбин Е. Ю., Косьянчук В. В. Синтез системы управления многосвязного объекта на основе технологии вложения // Автоматика и телемеханика. — 2002. — № 8. — С. 22–36.

REFERENCES

1. E. V. Gvozdev. Deviation algorithm for risk identification by a safety management system of the enterprise. *XXI vek. Tekhnosfernaya bezopasnost' / XXI century. Technosphere Safety*, 2018, vol. 3, no. 2(10), pp. 25–34 (in Russian). DOI: 10.21285/2500-1582-2018-2-25-34.
2. E. V. Gvozdev. Development of a method of detection and aggregation of the indicators of danger influencing subjects to protection of the enterprise and the environment. *XXI vek. Tekhnosfernaya bezopasnost' / XXI century. Technosphere Safety*, 2018, vol. 3, no. 3(11), pp. 69–81 (in Russian). DOI: 10.21285/1814-3520-2018-3-69-81.
3. E. V. Gvozdev. Analysis of reliability of complex enterprise technosphere safety systems based on destructive impact probabilities and destructive impact overcoming by the security subsystem. *XXI vek. Tekhnosfernaya bezopasnost' / XXI century. Technosphere Safety*, 2018, vol. 3, no. 4(12), pp. 51–66 (in Russian). DOI: 10.21285/1814-3520-2018-4-51-66.
4. E. V. Gvozdev. Validation of a centralized complex safety management method for technosphere safety objects. *XXI vek. Tekhnosfernaya bezopasnost' / XXI century. Technosphere Safety*, 2017, vol. 2, no. 4(8), pp. 97–107 (in Russian).
5. N. A. Makhutov, V. N. Permyakov, R. S. Akhmetkhanov, D. O. Reznikov, E. F. Dubinin. *Analiz riskov i obespecheniye zashchishchennosti kriticheski vazhnykh ob'ektov neftegazokhimicheskogo kompleksa* [Risk analysis and ensuring the security of critical facilities of a petrochemical complex]. Tyumen, Tyumen State Oil and Gas University Publ., 2013. 560 p. (in Russian).
6. I. Sutton. *Process risk and reliability management*. 2nd ed. Oxford, Gulf Professional Publishing, 2015. 798 p. Available at: <https://b-ok.org/book/2463300/b6cf53> (Accessed 1 December 2018).
7. *Assessment of large power transformer risk mitigation strategies*. Fairfax, ICF, October 2016. Available at: <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf> (Accessed 10 December 2018).
8. N. A. Makhutov, D. O. Reznikov, V. P. Petrov, V. I. Kuksova. Regulatory approaches to ensure safety of critical facilities. *Bezopasnost v tekhnosfere / Safety in Technosphere*, 2011, no. 4, pp. 5–12 (in Russian).
9. R. Billinton, R. N. Allan. *Reliability assessment of large electric power systems*. Boston, MA, Springer, 1988. DOI: 10.1007/978-1-4613-1689-3.
10. J. J. Popoola, A. A. Ponnle, T. O. Ale. Reliability worth assessment of electric power utility in Nigeria: Residential customer survey results. Available at: http://www.journal.au.edu/au_techno/2011/jan2011/journal143_article08.pdf (Accessed 10 December 2018).
11. S. Yu. Butuzov, A. Yu. Lyubavsky. Evaluation of mean time between failure of stores of information of automated systems fire and explosion safety. *Tekhnologii tekhnosfernoy bezopasnosti / Technology of Technosphere Safety*, 2011, issue 6(40) (in Russian). Available at: https://elibrary.ru/download/elibrary_20329697_28243844.htm (Accessed 1 December 2018).
12. A. Aneiba, M. Melad. Performance evaluation of AODV, DSR, OLSR, and GRP MANET routing protocols using OPNET. *International Journal of Future Computer and Communication*, 2016, vol. 5, no. 1, pp. 57–60. DOI: 10.18178/ijfcc.2016.5.1.444.
13. M. P. Bhavaraju, R. Billinton, R. E. Brown, J. Endrenyi, W. Li, A. P. Meliopoulos, C. Singh. IEEE tutorial on electric delivery system reliability evaluation. *IEEE Power Engineering Society (PES)*, 2005, Publication 05TP175, pp. 39–51.
14. N. G. Topolskii, S. Yu. Butuzov, E. N. Mineev. The automated system of prevention of emergency operation of electric motors at detection of currents of leak and short circuit. *Tekhnologii tekhnosfernoy bezopasnosti / Technology of Technosphere Safety*, 2015, issue 3(61), pp. 246–251 (in Russian). Available at: https://elibrary.ru/download/elibrary_25101416_29886300.pdf (Accessed 1 December 2018).
15. B. T. Abhilash, H. M. Manjunatha, N. A. Ranjan, M. E. Tejamoorthy. Reliability assessment of induction motor drive using failure mode effects analysis. *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, 2013, vol. 6, issue 6, pp. 32–36.

16. R. Billinton, W. Li. Reliability assessment of electric power systems using Monte Carlo methods. New York, London, Plenum Press, 1994. 351 p. DOI: 10.1007/978-1-4899-1346-3.
17. *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System*. Technical Report. Atlanta, NERC, November 2017. Available at: https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SPOD_11142017_Final.pdf (Accessed 10 December 2018).
18. M. A. Yastrebenetskiy, G. M. Ivanova. *Nadezhnost avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami* [Reliability control systems]. Moscow, Energoatomizdat, 1989. 264 p. (in Russian).
19. I. A. Birger. *Tekhnicheskaya diagnostika* [Technical diagnostics]. Moscow, Mashinostroyeniye Publ., 1978. 240 p. (in Russian).
20. E. V. Aref'eva, A. V. Rybakov, S. B. Arifdjanov. Evaluation of technogenic risk on the basis integral index. *Novosti nauki Kazakhstana / Science News of Kazakhstan*, 2018, issue 1(135), pp. 30–42 (in Russian).
21. L. A. Mironovskiy. *Funktsionalnoye diagnostirovaniye dinamicheskikh sistem* [Functional diagnostics of dynamic systems]. Moscow, Saint Petersburg, MGU-GRIF Publ., 1998. 256 p. (in Russian).
22. E. Yu. Zybin. On identifiability of closed-loop linear dynamical systems under normal operating conditions. *Izvestiya YuFU. Tekhnicheskiye nauki / Izvestiya SFedU. Engineering Sciences*, 2015, no. 4(165), pp. 160–170 (in Russian).
23. E. Yu. Zybin, V. V. Kos'yanchuk. An algebraic criterion for detecting the fact and time a fault occurs in control systems of dynamic plants. *Journal of Computer and Systems Sciences International*, 2016, vol. 55, no. 4, pp. 546–557. DOI: 10.1134/s1064230716040146.
24. E. Yu. Zybin. On the features of modeling and identification of discrete systems in the state space. In: *Upravleniye v tekhnicheskikh sistemakh* [Control in Technical Systems]. Proceedings of Conference. Saint Petersburg, GNTs RF – TsNII “Elektropribor” Publ., 2010, pp. 23–26 (in Russian).
25. E. Yu. Zybin, V. V. Kos'yanchuk. Design of the control system of a multivariable controlled plant using the embedding technology. *Automation and Remote Control*, 2002, vol. 63, no. 8, pp. 1225–1238. DOI: 10.1023/a:1019871124522.

Поступила 03.12.2018; после доработки 28.02.2019; принята к публикации 06.03.2019
Received 3 December 2018; received in revised form 28 February 2019; accepted 6 March 2019

Информация об авторах

ГВОЗДЕВ Евгений Владимирович, канд. техн. наук, старший преподаватель кафедры пожарной безопасности, Академия гражданской защиты МЧС России, Московская обл., г. Химки, Российская Федерация; e-mail: evgvozdev@mail.ru

БУТУЗОВ Станислав Юрьевич, д-р техн. наук, доцент, заслуженный работник высшей школы РФ, профессор кафедры информационных технологий, Академия ГПС МЧС России, г. Москва, Российская Федерация; e-mail: butuzov_s_yu@mail.ru

СУЛИМА Тимофей Геннадьевич, канд. воен. наук, начальник научно-исследовательского отдела, Академия гражданской защиты МЧС России, Московская обл., г. Химки, Российская Федерация; e-mail: sulima977@mail.ru

АРИФДЖАНОВ Султан Бахтиярович, канд. техн. наук, чл.-корр. Академии военных наук Республики Казахстан, профессор кафедры гражданской обороны и военной подготовки, Кокшетауский технический институт Комитета по чрезвычайным ситуациям МВД Республики Казахстан, г. Кокшетау, Республика Казахстан; e-mail: ayna_04112011@mail.ru

Information about the authors

Evgeniy V. GVOZDEV, Cand. Sci. (Eng.), Senior Lecturer of Fire Safety Department, Civil Defence Academy of Emercom of Russia, Moscow Region, Khimki, Russian Federation; e-mail: evgvozdev@mail.ru

Stanislav Yu. BUTUZOV, Dr. Sci. (Eng.), Associate Professor, Honoured Worker of Higher School of the Russian Federation, Professor of Information Technologies Department, State Fire Academy of Emercom of Russia, Moscow, Russian Federation; e-mail: butuzov_s_yu@mail.ru

Timofey G. SULIMA, Cand. Sci. (Military), Head of Research Department, Civil Defence Academy of Emercom of Russia, Moscow Region, Khimki, Russian Federation; e-mail: sulima977@mail.ru

Sultan B. ARIFJANOV, Cand. Sci. (Eng.), Corresponding Member of the Military Academy of Sciences of the Republic of Kazakhstan, Professor of the Department of Civil Defense and Military Training, Kokshetau Technical Institute of the Committee for Emergency Situations of the Ministry of Internal Affairs of the Republic of Kazakhstan, Kokshetau, Republic of Kazakhstan; e-mail: ayna_04112011@mail.ru