УДК 004.056

ПРЕЦЕДЕНТНЫЙ АНАЛИЗ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

В. Г. Жуков, А. А. Шаляпин

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Россия, 660014, Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: zhukov.sibsau@gmail.com, shalyapin2a@gmail.com

Рассматривается общий подход к управлению инцидентами информационной безопасности в соответствии с международным стандартом ISO/IEC 27001:2005 и его совершенствование путем автоматизации соответствующих процедур на этапе принятия решения при определении стратегии реагирования с помощью аппарата прецедентного анализа. Предлагаемый авторами подход основан на поиске решения по аналогии – от частного к частному. Приводится описание логической структуры, модели и алгоритма системы прецедентного анализа инцидентов, а также результаты численных экспериментов. Предложенная концепция построения системы прецедентного анализа инцидентов информационной безопасности позволит повысить оперативность реагирования и многократно использовать накопленный ранее опыт их разрешения в процессе автоматизированного управления инцидентами.

Ключевые слова: инцидент, прецедент, аналогия, стратегия реагирования, CBR-цикл.

CASE BASED ANALYSIS OF INFORMATION SECURITY INCIDENTS

V. G. Zhukov, A.A. Shalyapin

Siberian State Aerospace University named after academician M. F. Reshetnev
31 “Krasnoyarskiy Rabochiy” prosp., Krasnoyarsk, 660014, Russia
E-mail: zhukov.sibsau@gmail.com, shalyapin2a@gmail.com

The article considers the general approach to the management of information security incidents according to international standard ISO/IEC 27001:2005 and its improvement by means of corresponding procedures automation at the stage of decision making in the process of response strategy definition with the help of case based analysis apparatus. The approach proposed by the authors is based on finding solutions on the analogy – from specific to specific. The authors present description of the logical structure, the model and the algorithm of case based incidents analysis system, as well as the results of numerical experiments. The proposed concept of building the case based system of information security incidents will allow to increase responsiveness and to repetitively use the previous experience of their solution in the process of automated incidents management.

Keywords: incident, case, analogy, response strategy, CBR-cycle.

Всоответствиисмеждународнымстандартом ISO/IEC 27001:2005, управление инцидентами информационной безопасности является важным элементом в обеспечении непрерывности бизнес-процессов организации.Под управлением инцидентами понимается процесс, на вход которого подаются данные, полученные в результате протоколирования информации о событиях, имеющих отношение к информационной безопасности, а на выходе процесса получают информацию о причинах произошедшего инцидента и мерах, которые необходимо принять для того, чтобы инцидент не повторился.

В общем случае управление инцидентами – циклический процесс, основные стадии которого отображает модель PDCA (Plan-Do-Check-Act, модель непрерывного улучшения процессов). Согласно стандарту ISO 27001, классическая модель включает в себя четыре стадии управления: идентификацию инцидента информационной безопасности, реагирование на инцидент информационной безопасности, расследование, корректирующие и превентивные мероприятия [1].

Именно во время реагирования и расследования инцидентов проявляются конкретные уязвимости информационной системы, обнаруживаются следы атак и вторжений, проверяется работа средств защиты, качество архитектуры системы информационной безопасности и ее управления. Также важным является наличие процедур анализа и устранения последствий инцидентов и принятия корректирующих мер для снижения вероятности повторения подобных инцидентов в будущем.

В первую очередь необходимо своевременно обнаружить инцидент, иначе невозможно отреагировать на него в кратчайшие сроки. В то же время по инцидентам, которые все-таки удалось выявить, часто отсутствуют четкие процедуры реагирования. Подобные ситуации требуют значительного времени для разрешения.

* Работа поддержана грантом Президента РФ молодым кандидатам наук МК-473.2013.9.

Проблема реагирования на инциденты информационной безопасности. Основными средствами управления инцидентами являются системы мониторинга и корреляции событий информационной безопасности, автоматизирующие этап обнаружения инцидентов. Результаты работы данных средств анализируются экспертами, по результатам анализа разрабатываются стратегии реагирования. Большой объем информации, генерируемый системами мониторинга, требует наличия группы реагирования на инциденты информационной безопасности (ГРИБ), состоящей из квалифицированных специалистов. Далеко не всегда возможно эффективно организовать процесс управления инцидентами в силу финансовых ограничений и отсутствия штата специалистов. С другой стороны, полная зависимость от эксперта на этапе принятия решения снижает оперативность и, как следствие, увеличивает ущерб.

Таким образом, существует актуальная проблема оперативного реагирования на возникающие инциденты. Необходимо решить, какую стратегию из множества определенных применить, либо определить, что подходящей стратегии не существует и ее необходимо выработать.

Метод правдоподобного рассуждения позволит решить проблему реагирования на инциденты путем применения систем на основе прецедентов (Case-Based Reasoning, CBR) в качестве интегрированных средств автоматизации процесса управления. В итоге автоматизируется деятельность при определении стратегии реагирования на инциденты, что позволяет повысить эффективность, ускорить реакцию на возникающие инциденты и более интеллектуально подходить к процессу управления информационной безопасностью.

Прецедентный анализ. В прецедентных системах поиск решения базируется на понятии аналогии (поиск от частного к частному). Прецедент и текущая ситуация представляются объектами, для которых необходимо обнаружить аналогию и благодаря переносу фактов, справедливых для прецедента, сделать некоторое заключение относительно рассматриваемого инцидента. Как правило, прецедент состоит:

– из описания проблемной ситуации;

– совокупности действий, предпринимаемых для устранения данной проблемы (решения задачи);

– и в некоторых случаях – результата (или прогноза) применения решения [2; 3].

В качестве наиболее очевидной структуры прецедента можно привести параметрическое представление многомерным вектором:

$$CASE = (x_1, x_2, ..., x_p, R),$$

где $x_1, ..., x_p$ – параметры ситуации, описываемой данным прецедентом; R – одно или множество решений данной задачи (диагноз, рекомендации).

Вывод на основе прецедентов включает в себя четыре основных этапа, образующих CBR-цикл (цикл рассуждения на основе прецедентов) [2], которыми являются:

– извлечение подобных прецедентов для сложившейся ситуации из базы прецедентов;

– повторное использование прецедента для попытки решения текущей проблемы;

– пересмотр и адаптация решения в соответствии с текущей проблемой;

– сохранение вновь принятого решения как части нового прецедента.

С учетом специфики конкретной предметной области и решаемых задач может использоваться упрощенный CBR-цикл [4]. Таким образом, основная цель использования аппарата прецедентов заключается в выдаче готового решения оператору.

Извлечение прецедентов основывается на определении функции подобия (метрики) F, значение которой определяет сходство прецедента и текущей ситуации. В пространстве признаков определяется точка, соответствующая целевой проблеме, и в рамках используемой метрики выбирается ближайший прецедент. Формально аналогия прецедента $g = (x_{g1}, x_{g2}, ..., x_{gp})$ и текущей ситуации $k = (x_{k1}, x_{k2}, ..., x_{kp})$ описывается функцией вида

$$SIM\left(g,k\right) = F\left(sim(x_{g1}, x_{k1}), ..., sim(x_{gp}, x_{kp})\right),$$

где $sim(x_{gi}, x_{ki})$ – локальная схожесть значений i-го признака прецедента g и i-го признака текущей ситуации (инцидента) k. Функция F выражает полную схожесть прецедента с текущей ситуацией.

В случае отсутствия аналогичных прецедентов в базе данный подход не приведет к необходимому решению для возникшей ситуации. Данная проблема может быть разрешена, если в CBR-цикле будет предусмотрена возможность пополнения базы непосредственно в процессе рассуждения (вывода).

Концепция применения прецедентного анализа. Первым шагом управления инцидентами информационной безопасности, как отмечалось ранее, является непосредственно регистрация инцидентов. Дальнейшие действия предполагают применение стратегий реагирования для каждого инцидента с учетом класса. На данном этапе можно выделить следующие проблемы:

– не всегда классификация инцидентов производится корректно;

– не существует единой стратегии реагирования на инциденты определенного класса в силу того, что каждый инцидент в той или иной мере индивидуален;

– имеют место инциденты, не имевшие место ранее и, следовательно, для таких инцидентов отсутствуют подходящие стратегии реагирования.

Концепция применения прецедентного анализа для совершенствования процесса управления инцидентами заключается в следующем. Имеется множество G известных инцидентов, множество R определенных стратегий реагирования. Отображение $G \to R$ есть прецедент, т. е. пара, содержащая описание инцидента и соответствующей ему стратегии реагирования. При регистрации нового инцидента, для него находится подобный прецедент, после чего решение прецедента применяется для данного инцидента. Логическая структура системы, реализующей данный подход, приведена на рис. 1.

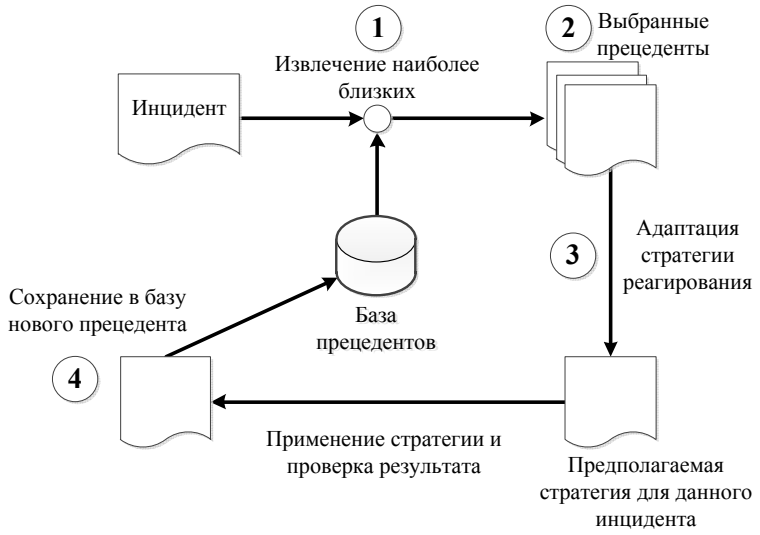

Рис. 1. Логическая структура системы прецедентного анализа

Инциденты, не известные ранее и для которых нет определенной стратегии реагирования, будем называть аномальными инцидентами. Другими словами, под аномальным инцидентом понимается инцидент, не имеющий аналогов в рамках класса, к которому он отнесен средством защиты. Заключение обаномальности инцидента дает повод для детального анализа.

С учетом этого прецедентный анализ сводится к классификации инцидентов на нормальные и аномальные исходя из количества найденных аналогий: $G = \{g_1, ..., g_n\}$ – множество прецедентов; $g_i = (x_1, ..., x_p, r_i)$ – единичный прецедент; $K = \{k_1, ..., k_m\}$ – множество зарегистрированных инцидентов; $k_j = (x_1, ..., x_p)$ – единичный инцидент; $F(g_i, k_j)$ – функция подобия; $G_1 = \{g_i : F(g_i, k_j) \le d_{\lim}\}$ – множество подобных прецедентов. Таким образом, условие отнесение инцидента к множеству прецедентов формулируется следующим образом:

$$k_j \in G \Leftrightarrow |G_1| \ge a_{\lim}.$$

Как видно, результат классификации напрямую зависит от предельного расстояния $d_{\lim}$ и предельного количества аналогий $a_{\lim}$.

Модель алгоритма прецедентного анализа. Для исследования эффективности предложенного подхода был использован источник данных KddDataset'99. В качестве метрического классификатора применялся метод *k*-ближайших соседей. Так как на данном этапе неизвестно влияние каждого параметра на конечный результат, то целесообразен выбор метрики без весовых коэффициентов.

Тестовый сценарий алгоритма реализован в аналитической платформе DeductorStudioAcademic и включает в себя следующие этапы (рис. 2):

1. После регистрации инцидента проводится его нормализация: $x_{\text{норм}} = \dfrac{x - x_{\min}}{x_{\max} - x_{\min}}$.

2. Инициализация параметров алгоритма: выбор метрики, определение предельного расстояние d_{lim} и предельного значения аналогий a_{lim}. В качестве начального значения d_{lim} принято расстояние по классу:

$$d_{cp} = \frac{\sum_{i=1}^{n} d_{i_{cp}}}{n},$$

где среднее расстояние единичного прецедента до класса

$$d_{i_{cp}} = \frac{\sum_{j=1}^{n} d_{ij}}{n-1}.$$

3. Расчет расстояний между объектами по метрики

$$d_{gk} = \sqrt{\sum_{i=1}^{p} \left(x_{gi} - x_{ki}\right)^2}.$$

4. Определение пар объектов, для которых справедливо $d_{gk} \le d_{lim}$ (прецедент g и инцидент k считаются подобными).

5. Для каждой инцидента k_j рассчитывается число a прецедентов, для которых выполняется $d_{gk} \le d_{lim}$.

6. Инцидент k_j рассматривается как аномалия при $a \le a_{lim}$.

7. Принимаются дальнейшие действия исходя из результата классификации: детальный анализ инцидентов либо применение стратегии реагирования, соответствующей наиболее аналогичному прецеденту.

Параметры алгоритма варьируются в ходе функционирования системы, за счет чего совместно с пополнением базы прецедентов реализуется обучение системы.

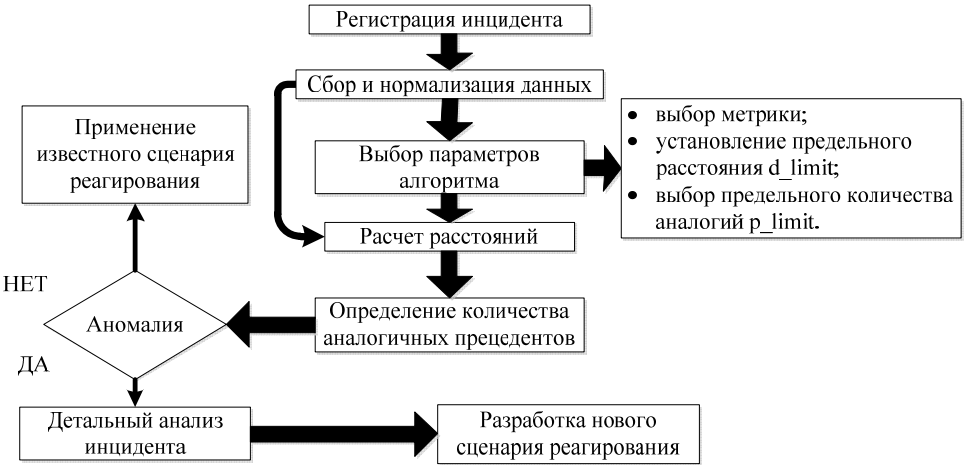

Рис. 2. Внедрение анализа инцидентов в процесс управления

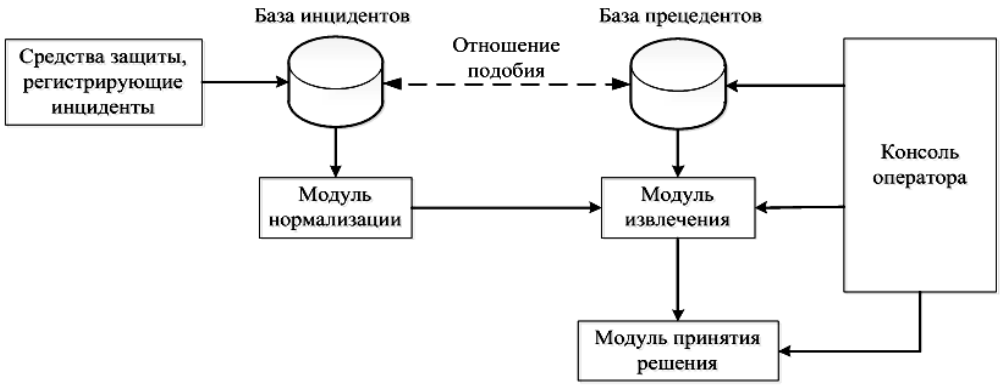

Рис. 3. Архитектура системы прецедентного анализа

Архитектура системы прецедентного анализа. С точки зрения программной реализации система прецедентного анализа имеет модульную структуру и включает в себя следующие компоненты (рис. 3):

1) базу инцидентов, содержащая записи о зарегистрированных инцидентах, ожидающих дальнейшей обработки;

2) модуль нормализации данных, преобразовывающий базу зарегистрированных инцидентов в соответствии со структурой базы прецедентов;

3) модуль извлечения, реализующий функцию расчета меры сходства инцидентов и прецедентов;

4) модуль принятия решений, определяющий результат классификации и ставящий инцидент в соответствие одному или нескольким прецедентам на основе рассчитанных мер подобия;

5) консоль оператора, предназначенная для коррекции процесса анализа и адаптации выработанной стратегии под ранее неизвестные условия.

Таким образом, применение предложенной концепции прецедентного анализа, в качестве инструмента, совершенствующего процесс управления инцидентами информационной безопасности, позволит повысить оперативность реагирования на инциденты, путем многократного применения накопленного опыт. Кроме того, данный подход позволяет решить задачу обнаружения аномальных инцидентов, являющихся наиболее критичными и требующих детального изучения.

Результаты численных экспериментов. Подобная реализация алгоритма позволяет получать результат как в аналитическом виде, так и в графическом, в виде точечной диаграммы. По точечной диаграмме визуально возможно определить аномалии – события, требующие внимания (рис. 4). Видно, что группа инцидентов, классифицированных как нормальные, отличаются по количеству аналогов от большинства нормальных инцидентов, т. е. имеют число аналогий, приближающееся к предельному. Это может также стать сигналом для проведения их детального анализа и выявления причин и скрытых факторов, в результате которых инциденты не укладываются в общую закономерность.

Пусть нулевая гипотеза представляет предположение о нормальности инцидента, тогда ошибкой 1-го рода является неверное опровержение нулевой гипотезы, ошибкой 2-го рода, неверное принятие нулевой гипотезы.

Выбор параметров $d_{\lim}$ и $a_{\lim}$ весьма противоречив. С одной стороны, увеличение предельного числа обнаруженных аналогий повышает достоверность классификации (снижает ошибки 1-го рода), но при этом границы между классами становятся менее четкими. Уменьшение же предельного расстояния также приводит к более точной классификации, но увеличивает вероятность ошибок 2-го рода (рис. 5). Как видно, один нормальный инцидент классифицирован неверно.

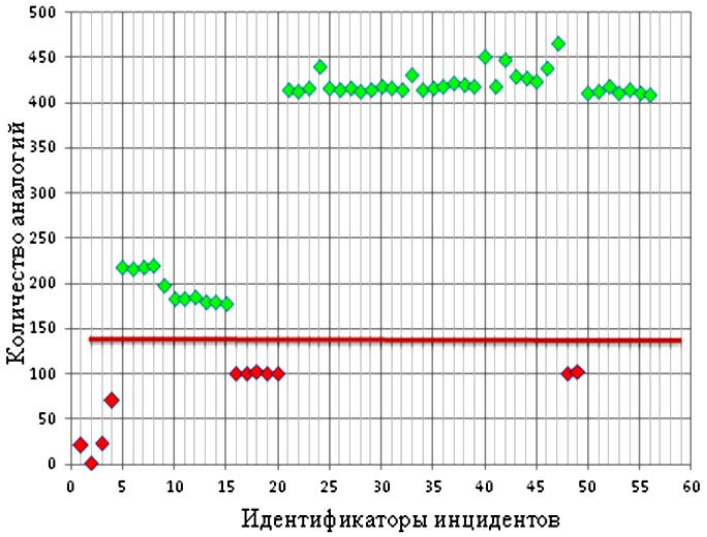

Рис. 4. Результат классификации инцидентов

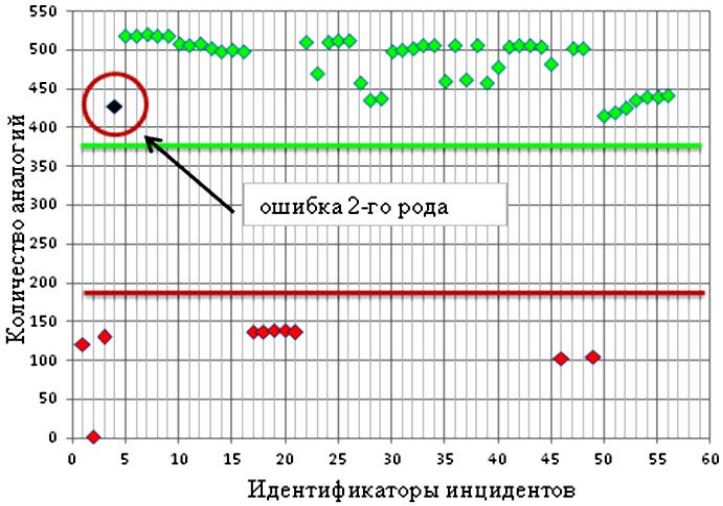

Рис. 5. Результат классификации инцидентов

Параметр a_{lim} зависит от конкретной ситуации. Предложенный подход классификации инцидентов для поиска аномалий сочетает в себе высокую точность обнаружения и низкий уровень ложных срабатываний, что достигается путем индивидуального выбора параметров алгоритма для каждого класса инцидентов.

Преимущества применения прецедентного анализа заключаются в возможности повторно применять накопленный опыт и в сокращении времени поиска сценариев реагирования для аналогичных инцидентов. Предложенная концепция позволяет решить задачу обнаружения аномальных инцидентов, требующих детального изучения сложившейся ситуации, и автоматизировать процесс получения решения для инцидентов, знания о которых содержатся в базе прецедентов.

Библиографические ссылки

1. ISO/IEC 27001:2005 Information technology – Security Techniques – Information Security Management Systems – Requirements.

2. Aamodt A., Plaza E. Case-Based Reasoning: Foundational Issues, methodological Variations, and System Approaches // AI Communications. 1994. Vol. 7, № 1. P. 39–59.

3. Люгер Д. Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. М. : Вильямс, 2002.

4. Концепция построения прецедентной экспертной системы / А. Ф. Берман, О. А. Николайчук, А. И. Павлов, А. Ю. Юрин // Материалы XII Междунар. конф. по вычисл. механике и соврем. прикл. прогр. системам. М., 2003. Т. 2. С. 110–111.

References

1. ISO/IEC 27001:2005 Information technology – Security techniques – Information Security Management Systems – Requirements.

2. Aamodt A., Plaza E. Case-Based reasoning: Foundational issues, methodological variations, and system approaches. AI Communications, 1994, vol. 7, no. 1, pp. 39–59.

3. Lyuger D. F. *Iskusstvennyj intellekt: strategii i metody resheniya slozhnyx problem* (Artificial Intelligence: Strategies and methods to solvedifficult problems). Moscow, Vilyams, 2002.

4. Berman A. F., Nikolajchuk O. A., Pavlov A. I., Yurin A. Yu. *Materialy XII mezhdunarodnoj konferencii po vychislitelnoj mexanike i sovremennym prikladnym programmnym sistemam* (Materials XII Intern. Conf. on ComputationalMechanics andAdvanced Applied). Vladimir, June 30 – July 5, 2003. Moscow, vol. 2, pp. 110–111.

© Жуков В. Г., Шаляпин А. А., 2013

УДК 621.31:681.5

СИНТЕЗ ОПТИМАЛЬНЫХ ПО БЫСТРОДЕЙСТВИЮ СИСТЕМ ВЫСОКОГО ПОРЯДКА

Д. В. Замятин[1], А. Н. Ловчиков[2]

[1]Сибирский федеральный университет
Россия, 660074, Красноярск, ул. Академика Киренского, 28. E-mail: zamyatin@mail.ru
[2]Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Россия, 660014, Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: ivt_anlovch@sibsau.ru

Исследованы возможности синтеза систем автоматического регулирования, описываемых системами дифференциальных уравнений третьего и четвертого порядка, оптимальных по быстродействию. Выполнен анализ существующих разработок для создания систем высокого порядка, оптимальных по быстродействию. Представлена простая методика синтеза, основанная на методе фазовых траекторий. Предлагаемая методика включает в себя все этапы создания оптимальной по быстродействию системы от исходного описания в виде дифференциального уравнения или передаточной функции до формирования корректирующего звена. Сложность создания системы высокого порядка, оптимальной по быстродействию, заключается в необходимости иметь для управления информацию о n – 1 производных, где n – порядок системы дифференциальных уравнений. Однако технически получить такую информацию практически невозможно. Предлагается способ создания устройства для получения необходимой информации при синтезе систем высокого порядка, оптимальных по быстродействию.

Ключевые слова: оптимальные системы, метод фазовых траекторий, быстродействующие системы.

SYNTHESIS OF TIME OPTIMAL SYSTEMS OF HIGH ORDER

D. V. Zamjatin[1], A. N. Lovchikov[2]

[1]Siberian Federal University
28 Kirenskiy st., Krasnoyarsk, 660074, Russia. E-mail: zamyatin@mail.ru
[2]Siberian State Aerospace University named after academician M. F. Reshetnev
31 “Krasnoyarskiy Rabochiy” prosp., Krasnoyarsk, 660014, Russia. E-mail: ivt_anlovch@sibsau.ru

The purpose of the work is to study the possibility of the synthesis of systems of automatic control described with time optimal systems of differential equations of the third and the fourth order. The authors analyze the existing investigations for creation of time optimal systems of high order and present a simple synthesis strategy based on the method of the phase trajectories. The proposed strategy includes all the stages of creation of the time optimal system, from the input description in the form of a differential equation or a transfer function to formation of a correcting section. The creation of time optimal system of higher-order is challenging to obtaining the information about the n – 1 derivatives, where n is the order of the system of differential equations. However, to obtain such information technically is practically impossible. The article proposes a way to create a device for obtaining the necessary information with the synthesis of time optimal systems of high order.

Keywords: optimal system, method of phase trajectories, time optimal systems.