УДК 681.5

МОДЕЛЬ НАДЕЖНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Гладких Т.Д.

ФГБОУ ВО «Тюменский индустриальный университет», Тюмень, e-mail: txgl@yandex.ru

В статье представлена модель надежности автоматизированной системы управления технологическим процессом (АСУ ТП) в период эксплуатации. Предложенная модель построена на основе сети Байеса, что позволяет графически передать архитектуру АСУ, и предназначена для выявления уязвимых элементов системы. Основанием применения сети Байеса для моделирования является необходимость комплексного рассмотрения принципиально различных подсистем: аппаратных средств и программного обеспечения (ПО). Для формирования сети Байеса отдельно получены функции надежности для всех составляющих элементов АСУ: каналов связи в аппаратной части и программных средств системы управления. В качестве показателя надежности использована вероятность безотказной работы системы, которая описывается экспоненциальным законом распределения наработки до отказа. При получении функции надежности (вероятности безотказной работы) программного обеспечения применялась модель Джелинского – Моранды. Данная модель наиболее подходит нашему случаю, так как позволяет рассматривать систему в процессе эксплуатации. Для расчета вероятности безотказной работы ПО использованы данные по наработке между сбоями программного обеспечения средств автоматизации среднего и верхнего уровня реального технологического объекта. Модель безотказности аппаратной части АСУ ТП построена на основе структурных схем. Аппаратная составляющая системы управления рассматривается с учетом уровней автоматизации: нижнего, среднего и верхнего. Для каждого уровня выделены каналы связи, для которых определены средняя интенсивность отказов и вероятность безотказной работы.

Ключевые слова: надежность программно-аппаратных систем, вероятность безотказной работы, модель Джелинского – Моранды, структурные схемы надежности, динамическая сеть Байеса

THE DEPENDABILITY MODEL OF THE IDUSTRIAL CONTROL SYSTEM

Gladkikh T.D.

Industrial University of Tyumen, Tyumen, e-mail: txgl@yandex.ru

The article presents a dependability model of an Industrial Control System (ICS) during operation. The proposed model is based on the Bayes network, which allows to graphically convey the architecture of the control system. The model is designed to identify vulnerable elements of the system. The basis for the use of the Bayes network for modeling is the need for a comprehensive consideration of fundamentally different subsystems: hardware and software. To form a Bayesian network, reliability functions were separately obtained for all the components of the control system: communication channels in the hardware and software of ICS. As an indicator of dependability, the reliability function of the system is used, which is described by the exponential law of the distribution of operating time to failure. The Jelinsky – Moranda model was used to obtain the reliability function of the software. This model is most suitable for our case, as it allows us to consider the system during operation. The reliability function of the software is calculated based on the operating time between failures. Failures at the controller and control room level are taken into account. The dependability model of the control system hardware is based on structural schemes. The hardware component is considered taking into account the levels of automation: lower, middle (controller) and upper (control room). Communication channels are allocated for each level, for which the average failure rate and the reliability function are determined.

Keywords: dependability of software and hardware systems, reliability function, Jelinsky – Moranda model, structural schemes, dynamic Bayesian network

Анализ надежности технических объектов позволяет оценить эффективность их работы и выявить уязвимые элементы в системах. Поэтому разработка моделей и методик оценки показателей безотказности является актуальной научно-технической задачей.

Для организаций, эксплуатирующих и проектирующих технические системы, существует необходимость в универсальной интегрированной среде моделирования надежности [1]. Как отмечают авторы статьи [1], для разработки такой среды необходима обширная библиотека разного рода моделей надежности.

Выбор методов оценки надежности технических систем необходимо осуществлять с учетом специфики анализируемого объекта [2]. Например, в работе [3] отмечается, что для инженеров необходим инструмент оценки надежности, в котором бы отражалась архитектура самого объекта. Модель надежности системы управления не может быть универсальной, так как необходимо учитывать не только архитектуру объекта, но и цель моделирования, доступные данные и др. Так, при разработке моделей надежности систем управления в работах [4, 5] объект исследования был разбит на подсистемы с учетом выполняемых функций.

Известным способом анализа надежности систем управления является применение метода анализа видов и последствий отказов (FMEA) [6, 7], но указанный ин-

струмент не является достаточным и рассматривается как начальный этап оценки безотказности и безопасности объекта на этапе проектирования [8].

Предложенная нами модель рассматривает АСУ ТП в период эксплуатации. Но авторы [1, 3] отмечают, что оценка надежности эксплуатируемых объектов усложнена тем, что показатели надежности являются динамическими, и, следовательно, модель надежности должна использовать данные текущего момента функционирования объекта. Для решения данной проблемы в [1] предлагается метод, основанный на динамической байесовской сети, которая представляет типовую сеть Байеса в функции времени. В рассматриваемом методе время является еще одним рядом данных. Кроме того, применение динамических сетей Байеса позволяет просто и наглядно моделировать надежность и безопасность сложных объектов [9]. С учетом вышесказанного, при разработке модели надежности АСУ ТП необходимо учитывать функциональное назначение составляющих элементов (программные и аппаратные средства), архитектуру (нижний, средний и верхний уровни автоматизации) и динамику изменений в системе (суммарную наработку).

Целью исследования является разработка модели функциональной надежности АСУ ТП. При расчете функциональной надежности учитываются функциональные отказы, под которыми понимаются состояния объекта, при которых система не выполняет какую-либо функцию, например не осуществляет контроль или регистрацию технологического параметра. При функциональном отказе система может быть работоспособной.

Материалы и методы исследования

При моделировании надежности АСУ ТП используем динамическую сеть Байеса, которая позволяет интегрировать модели надежности двух подсистем: программной и аппаратной составляющих системы управления. Для создания сети в нашем случае узлы описываются математическими моделями в функции времени.

При разработке модели выделяем программную и аппаратную части, в последней учитываем уровни автоматизации (нижний, средний, верхний). Для указанных подсистем применяются различные средства анализа безотказности. Поэтому вначале создаем отдельно модель надежности программного обеспечения и модель надежности аппаратных средств (с выделением уровней автоматизации), в завершение объединяем полученные модели подсистем в динамическую сеть Байеса.

Модель надежности программных средств. Модель надежности программного обеспечения является частью модели надежности АСУ ТП. Для оценки надежности ПО применяются аналитические и эмпирические методы; используют математический аппарат теории вероятности [10] и математической статистики, теории Марковских цепей [11] и др. [12].

Так как создаваемая модель надежности АСУ ТП динамическая, то и модель надежности ПО должна быть динамической, например, базироваться на модели Шумана или Джелинского – Моранды.

Динамическая модель Шумана в нашем случае непригодна, так как требует знания числа команд на машинном языке в программе; в нашем случае такие данные получить проблематично, так как необходимо учесть ПО среднего и верхнего уровня автоматизации. Безусловно, модель Шумана при наличии исходных данных очень удобна.

Таким образом, при разработке модели надежности ПО использовали модель Джелинского – Моранды [13–15].

Модель Джелинского – Моранды использует данные о периодичности возникновения программных сбоев, которые легко отследить в процессе эксплуатации, и является «моделью роста надежности», так как при исправлении ошибок надежность ПО увеличивается. Данная модель при описании показателей безотказности использует экспоненциальный закон распределения. Функция надежности ПО имеет вид $P(t_i) = \exp(-\lambda_i \cdot t_i)$, где t_i – момент времени после очередного $(i-1)$-го восстановления; λ_i – интенсивность отказов (сбоев) программы на i-м интервале работы. Методика расчета интенсивности отказов ПО подробно изложена в литературе, например в [14].

Пример расчета. Для определения интенсивности отказов использованы данные за 198 суток (6,6 мес.) АСУ ТП дожимной насосной станции Южно-Аганского месторождения. Исходные данные по наработке получены с момента обновления ПО, составляют $\tau = [12, 30, 35, 37, 41, 43]$, сут. Возникшие после модернизации АСУ ошибки устранялись перезагрузкой ПО и внесением незначительных корректив в код. Ошибки (сбои) ПО, возникшие в течение суток после модернизации системы, не учтены как возникшие в результате пуско-наладочных мероприятий.

На основе данных рассчитана интенсивность отказов ПО на $i = 7$ интервале эксплуатации, она составила $\lambda_7 = 0{,}015$ (1/сут). Функция вероятности безотказной работы (функция надежности) ПО на 7-интервале эксплуатации имеет вид: $P(t) = \exp(-0{,}015 \cdot t)$.

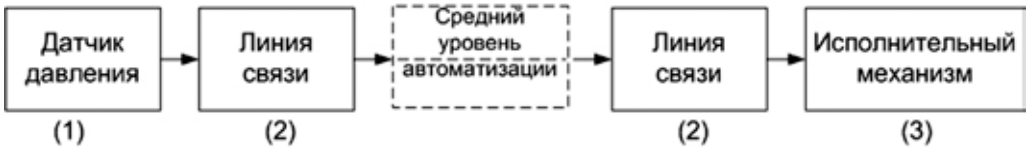

Рис. 1. Структурная схема надежности канала связи по давлению

Модель надежности аппаратных средств. Для описания надежности аппаратных средств применяли метод, основанный на структурных схемах. При разработке структурных схем и математического описания надежности приняли следующие допущения:

– отказ любого элемента вызывает функциональный отказ АСУ ТП, то есть система не выполняет все требуемые функции;

– АСУ рассматривается в период нормальной эксплуатации, то есть для описания показателей безотказности элементов можно применять экспоненциальный закон распределения. Предельное состояние объекта не рассматриваем, так как в процессе эксплуатации АСУ ТП постоянно модернизируется или выполняется восстановление при проведении планового технического обслуживания (ТО) и ремонта; кроме того, составляющие АСУ элементы, как правило, неремонтопригодны, после отказа заменяются исправными;

– средства противоаварийной защиты (ПАЗ) не рассматриваются.

В связи с первым допущением отмечаем, что структурная схема надежности канала связи представляет собой основное (последовательное) соединение элементов. Упрощенная структурная схема для каналов связи нижнего уровня имеет вид: датчик – линия связи – исполнительный механизм. Для среднего/верхнего уровня: контроллер – линия связи – автоматизированное рабочее место (АРМ). Для примера на рис. 1 изображена структурная схема канала регулирования по давлению.

Для получения функции надежности каналов связи рассчитывается интенсивность отказов элементов по формуле $\lambda_i = 1/T_i$, где T_i – средняя наработка до отказа (определяется из паспортов оборудования). Интенсивность отказов канала связи определяется суммой $\lambda_C = \sum \lambda_1$, так как структурная схема надежности описывается основным соединением элементов.

Вероятность безотказной работы канала связи имеет вид:

$$P_i(t) = e^{-\lambda_{CP} \cdot t}.$$

Рассмотрим расчет надежности для АСУ дожимной насосной станции Южно-Аганского месторождения. На объекте функционируют сепарационные установки, насосный блок с двумя насосными агрегатами.

На основе структурной схемы канала регулирования давления в сепараторе (РС) (рис. 1) определена интенсивность отказов:

$$\lambda_{CP} = \lambda_1 + 2\lambda_2 + \lambda_3 =$$

$$= 1 \cdot 10^{-5} + 2 \cdot 0.033 \cdot 10^{-5} + 1,7 \cdot 10^{-5} =$$

$$= 2.766 \cdot 10^{-5} \ (час^{-1}).$$

Вероятность безотказной работы канала регулирования давления описывается выражением $P_{PC}(t) = e^{-\lambda_{CP} \cdot t} = e^{-2.766 \cdot 10^{-5} \cdot t}$.

Аналогичным образом рассчитываются показатели безотказности для других каналов связи:

– канал регулирования уровня в сепараторе (LC) $P_{LC}(t) = e^{-2.167 \cdot 10^{-5} \cdot t}$;

– канал сигнализации по давлению в сепараторе (PA) $P_{PA}(t) = e^{-1.346 \cdot 10^{-5} \cdot t}$;

– канал контроля давления на выкиде насоса (PI) $P_{PI}(t) = e^{-2.806 \cdot 10^{-5} \cdot t}$;

– канал контроля температуры подшипников насоса (TI) (2 шт.) $P_{TI}(t) = e^{-3.01 \cdot 10^{-5} \cdot t}$;

– канал среднего/верхнего уровня (ПЛК+АРМ) $P_{ПЛК+АРМ}(t) = e^{-2.533 \cdot 10^{-5} \cdot t}$.

При разработке динамической модели надежности аппаратных средств принято следующее:

– техническое обслуживание (ТО) для элементов нижнего уровня автоматизации выполняется одновременно с периодичностью 6 мес. (согласно НТД техническое обслуживание должно проводиться не реже 1 раза в 5–7 мес.);

– периодичность ТО для средств автоматизации среднего и верхнего уровней составляет 12 мес.;

– после аварийного восстановления или ТО достигается исправное состояние системы;

– восстановление происходит мгновенно.

В примере расчета из-за отсутствия данных не учтены аварийные отказы и восстановления после них.

На рис. 2 представлены графики функции надежности для выделенных каналов связи АСУ на интервале наработки 135–240 суток.

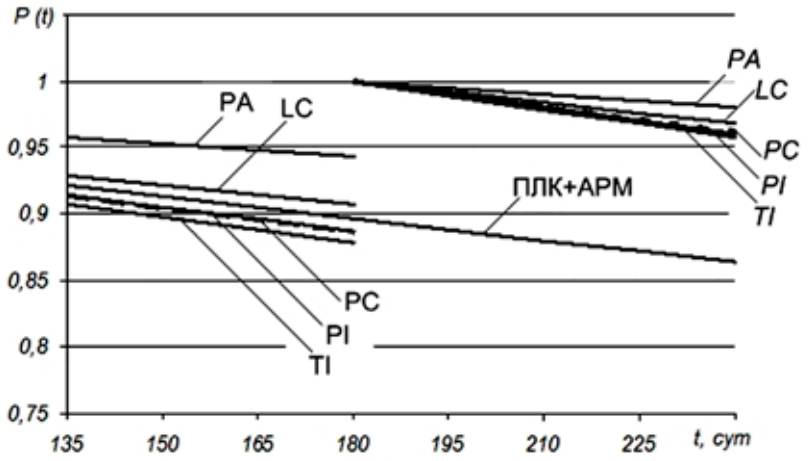

Рис. 2. Функция надежности для аппаратных средств АСУ

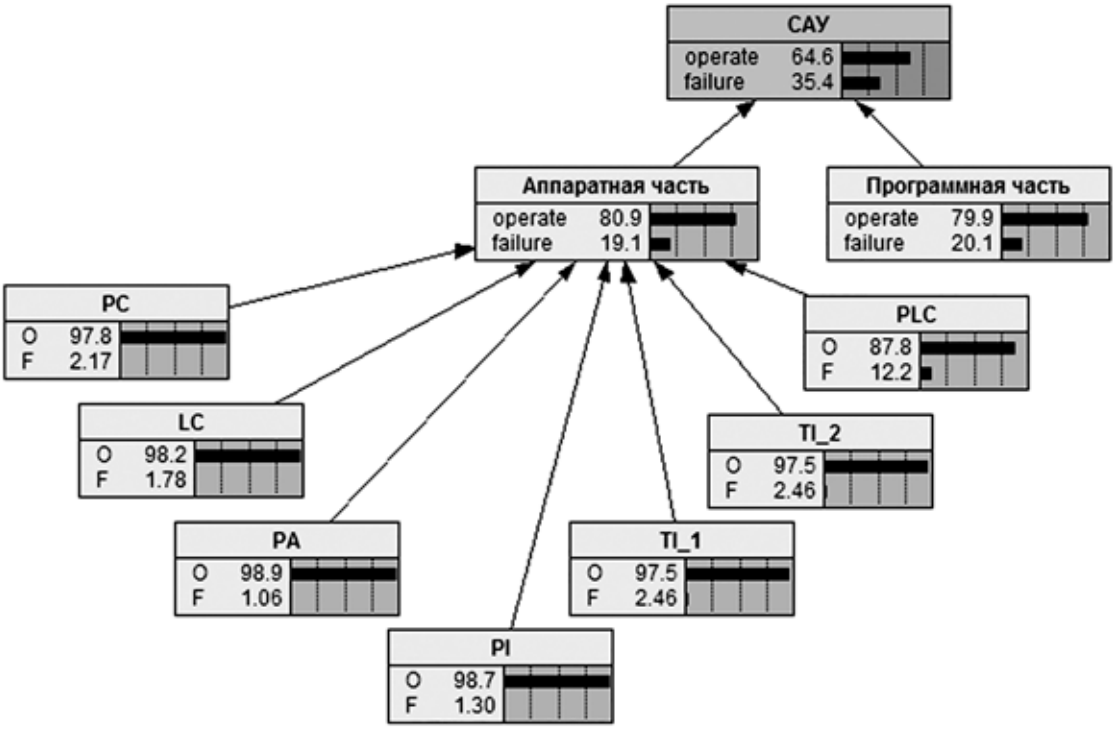

Рис. 3. Сеть Байеса для АСУ ДНС при наработке 213 суток

По графикам видно, что при наработке 180 суток (6 мес.), после планового ТО, каналы связи нижнего уровня восстановлены полностью: ($P_{PC}(180) = P_{LC}(180) = P_{PA}(180) = P_{PI}(180) = P_{TI}(180) = 1$); при увеличении наработки надежность снижается. Подсистема «ПЛК+АРМ» не восстанавливается на рассматриваемом интервале эксплуатации, ее надежность снижается на данном интервале.

Модель надежности АСУ ТП на базе динамической сети Байеса. Для оценки безотказности АСУ дожимной насосной станции Южно-Аганского месторождения разработана динамическая сеть Байеса, исходные данные для которой определяются по разработанным моделям надежности ПО и аппаратных средств. Из полученных выше моделей надежности для ПО и аппаратных средств используются выражения функции надежности вида $P_i(t) = \exp(\lambda_1 \cdot t)$, где i – элемент системы.

На рис. 3 представлена сеть Байеса с данными для момента непрерывной работы 213 суток (15 суток 7-го интервала работы ПО).

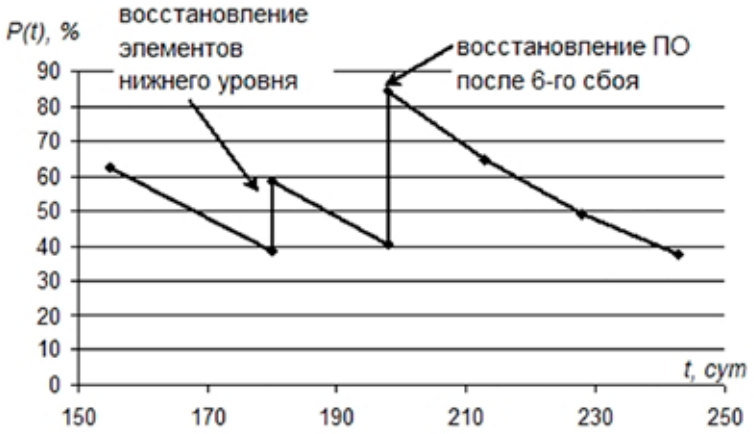

Рис. 4. График функции надежности АСУ ТП

На рисунке 3 использованы следующие обозначения: «O/operate» – вероятность безотказной работы объекта, «F/failure» – вероятность отказа объекта. Для данного момента времени наименьшим значением вероятности безотказной работы характеризуется ПО $P_{ПО}(213) = 79.9\%$, то есть с большой вероятностью может произойти сбой; среди аппаратных средств наиболее уязвимым местом АСУ является канал связи среднего/верхнего уровня (PLC) $P_{PLC}(213) = 87.7\%$.

На основе предложенной сети Байеса можно определить вероятность безотказной работы АСУ ТП в функции наработки. На рис. 4 представлен график изменения функции надежности АСУ ТП на интервале наработки 150–250 суток после модернизации. На диаграмме отражено восстановление элементов системы управления при ТО аппаратных средств нижнего уровня автоматизации (при 180 сутках) и после 6-го сбоя программного обеспечения (при 198 сутках).

Заключение

В статье предложена модель надежности, которая позволяет комплексно оценивать безотказность программно-аппаратной системы, какой является АСУ ТП. Разработанная модель является динамической и позволяет оценивать функцию надежности в процессе эксплуатации технических объектов.

Предложенная модель надежности рассматривает аппаратно-програмную систему в период нормальной эксплуатации, при которой отсутствуют износовые отказы. Тем не менее данную модель можно применить и для процесса приработки и для периода старения системы: в этом случае необходимо применить логнормальное или распределение Вебулла для описания наработки до отказа аппаратных средств.

Достоинствами разработанной модели являются: соблюдение архитектуры АСУ, визуальная реализация в виде сети Байеса, простота получения данных для модели, учет динамики изменения показателей надежности во времени.

Предложенную модель в дальнейшем можно уточнить следующими способами:

− расчетом интенсивности отказов аппаратных средств на основе статистических данных;

− выделением уровней автоматизации для ПО;

− выделением в модели надежности ПО различного типа сбоев, в том числе нарушения безопасности.

Список литературы

1. Qian W., Liu J., Cao Q., Yin X., Xie L. Reliability assessment of car engine based on dynamic Bayesian network, 2016 11th International Conference on Reliability, Maintainability and Safety (ICRMS). 2016. P. 1–4. DOI: 10.1109/ICRMS.2016.8050144.

2. Reza H., Pimple M., Krishna V., Hildle J. A Safety Analysis Method Using Fault Tree Analysis and Petri Nets, 2009 Sixth International Conference on Information Technology: New Generations, 2009. P. 1089–1094. DOI: 10.1109/ITNG.2009.183.

3. Boyer G., Pétin J., Brînzei N., Camerini J., Ndiaye M. Toward Generation of Dependability Assessment Models for Industrial Control System, 2019 International Conference on Information and Digital Technologies (IDT). 2019. P. 50–59. DOI: 10.1109/DT.2019.8813373.

4. Andrii A., Ol'ha B., Sergii N. Probabilistic evaluating the reliability of the control system of the unmanned aviation complex, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. P. 353–357. DOI: 10.1109/DESSERT.2018.8409158.

5. Успенский М.И. Вклад составляющих в надежность функционирования информационной сети СМПР // Известия Российской академии наук. Энергетика. 2021. № 3. С. 103–121. DOI: 10.31857/S0002331021020138.

6. Kong S., Zhang H., Liao X., Hong D. Reliability-centered optimal design method for flight vehicle control system, 2016 11th International Conference on Reliability, Maintainability and Safety (ICRMS), 2016. P. 1–6. DOI: 10.1109/ICRMS.2016.8050056.

7. Babeshko E., Kharchenko V., Gorbenko A. Applying F(I)MEA-technique for SCADA-Based Industrial Control Systems Dependability Assessment and Ensuring," 2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, 2008. P. 309–315. DOI: 10.1109/DepCoS-RELCOMEX.2008.23.

8. Bluvband Z., Grabov P. Failure analysis of FMEA, 2009 Annual Reliability and Maintainability Symposium, 2009. P. 344–347. DOI: 10.1109/RAMS.2009.4914700.

9. Li N., Lu Z., Zhou J. Reliability assessment based on Bayesian networks for full authority digital engine control systems, 2016 11th International Conference on Reliability, Maintainability and Safety (ICRMS), 2016. P. 1–7. DOI: 10.1109/ICRMS.2016.8050158.

10. Ермаков А.А., Чувашова Д.А. Особенности комплексного оценивания надежности программного обеспечения // Информационные технологии и проблемы математического моделирования сложных систем. 2016. № 15. С. 12–17.

11. Sun L., Gao S., Wang L. An Automatic Test Sequence Generation Method Based on Markov Chain Model. 2021. World Conference on Computing and Communication Technologies (WCCCT). 2021. P. 91–96. DOI: 10.1109/WCCCT52091.2021.00024.

12. Любицын В.Н. Необходимость разработки надежного программного обеспечения как вызов современности // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2012. № 23 (282). С. 26–29.

13. Гуров В.В. Практические особенности использования моделей надежности программного обеспечения // Вестник Национального исследовательского ядерного университета МИФИ. 2017. Т. 6. № 5. С. 458–465. DOI: 10.1134/S2304487X17050030.

14. Joe H., Reid N. On the Software Reliability Models of Jelinski-Moranda and Littlewood, in IEEE Transactions on Reliability. 1985. Vol. R-34. No. 3. P. 216–218. DOI: 10.1109/TR.1985.5222120.

15. Luo Z., Cao P., Tang G., Wu L. A Modification to the Jelinski-Moranda Software Reliability Growth Model Based on Cloud Model Theory. 2011 Seventh International Conference on Computational Intelligence and Security. 2011. P. 195–198. DOI: 10.1109/CIS.2011.51.