ВЕСТНИК НАЦИОНАЛЬНОГО ИССЛЕДОВАТЕЛЬСКОГО ЯДЕРНОГО УНИВЕРСИТЕТА “МИФИ”, 2021, том 10, № 5, с. 429–435

ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

УДК 681.5

ОСНОВНЫЕ АСПЕКТЫ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМ УПРАВЛЕНИЯ

© 2021 г. А. А. Звонарева[1,*], А. О. Толоконский[1,]**

[1] Национальный исследовательский ядерный университет “МИФИ”, Москва, 115409, Россия

**e-mail: AAZvonareva@mephi.ru*

***e-mail: toloconne@yandex.ru*

Поступила в редакцию 20.12.2021 г.
После доработки 21.12.2021 г.
Принята к публикации 30.12.2021 г.

Одним из важнейших показателей качества является надежность изделия. Поскольку программное обеспечение является неотъемлемой частью АСУ ТП, то отказ программных компонентов является причиной серьезного ухудшения надежности изделия и может вызвать потерю требуемой функции. В данной работе представлена характеристика основных источников отказов программно-аппаратных комплексов в атомной промышленности и рассмотрены методы предупреждения неисправностей. Тем не менее, опыт создания ПО позволяет выделить наиболее часто встречающиеся ошибки при его проектировании. К укрупненным причинам отказов программного обеспечения можно отнести такие причины, как несовершенство технического задания на программирование, ошибки программиста, разрабатывающего программные модули, ошибки эксплуатационного персонала, использующего ПО, изменение условий эксплуатации ПО, возможность появления недопустимых арифметических операций, недостаточно полный анализ свойств системы в составе которой функционирует ПО. Ошибки, допускаемые при программировании, не всегда быстро могут быть замечены при анализе текста программного модуля (ПМ). Особенно это касается ПМ, в которых имеются сложные логические операции. Поэтому при верификации следует руководствоваться документами, предназначенными для обеспечения качества ПМ, в которых имеются рекомендации по использованию типовых программных конструкций, размеров программных модулей и т.д.

Ключевые слова: надежность, отказ, причина, ПО, валидация, верификация

DOI: 10.1134/S2304487X21050126

ВВЕДЕНИЕ

Всякое изделие (транспортное средство, система управления, ЭВМ, двигатели и другие элементы сложных устройств и т.д.) являются, как правило, продуктом человеческой деятельности, поэтому изготовление изделия тесно связано с многочисленными этапами этой деятельности:

– предварительными научными исследованиями, на основании которых выявляется возможность создания изделия;

– разработкой технического задания, в котором перечисляются выполняемые изделием функции и требования к ним;

– эскизным и техническим проектированием, конечным результатом которого является полное описание создаваемого изделия;

– рабочим проектированием, в результате которого появляется головной образец изделия;

– испытанием и опытной эксплуатацией изделия, в процессе которых выявляются недостатки изделия и принимаются меры по устранению недостатков;

– авторский надзор, предназначенный для недопущения неквалифицированного вмешательства в изменение изделия и возможности улучшения характеристик изделия на основе накопленного опыта промышленной эксплуатации.

Перечисленные этапы составляют основу жизненного цикла изделия. На каждом этапе непременно присутствует человеческая деятельность. Поэтому следует признать, что большинство дефектов, показатели качества и свойства изделия теснейшим образом связаны с человеческим фактором.

Какие же ошибки допускаются людьми. Можно перечислить некоторые характерные ошибки для рассмотренных этапов:

– неадекватное или неполное описание процессов, которые будут происходить при эксплуатации предполагаемого изделия, на этапе научных исследований;

– не достаточно четкая формулировка в техническом задании необходимого перечня функций и требований к ним;

– отсутствие должной информации о свойствах и характеристиках структурных элементов изделия на этапе технического проектирования;

– ошибки, допускаемые эксплуатационным персоналом по невнимательности или недостаточной подготовленности.

Как показывает практика, все многообразие ошибок вряд ли можно перечислить. Но совершенно очевидно, что необходимо на каждом этапе предпринимать меры для их уменьшения и устранения.

В данной работе представлена характеристика основных источников отказов программно-аппаратных комплексов в атомной промышленности и рассмотрены методы предупреждения неисправностей.

ОБЩАЯ ПРОБЛЕМА НАДЕЖНОСТИ

Как уже было отмечено ранее, большое количество свойств изделия связано с возможностью возникновения ошибки, допущенной человеком. Поскольку рассматриваемый вопрос не является новым, то к настоящему времени уже выработаны некоторые меры по уменьшению числа ошибок на ранних этапах жизненного цикла изделий. К числу этих мер, например, относятся:

– необходимость обсуждения достигнутых результатов на совещаниях, научных конференциях, опубликование результатов в научных журналах и т.д.;

– выполнение требований правильной последовательности разработки изделий, которые излагаются в руководящих документах (ГОСТах, отраслевых стандартах, стандартах предприятия и т.д.);

– создание стандартов по обеспечению качества;

– рекомендации по созданию на предприятиях системы обеспечения качества;

– создание специальных рекомендательных стандартов при изготовлении элементов систем;

– использование процедур верификации и валидации при разработке программных продуктов;

– требования к обучению персонала, ведущего эксплуатацию.

Одним из важнейших показателей качества, используемым в атомной отрасли является надежность изделия. Надежность – это способность выполнять изделием возложенные на него функции в течение заданного интервала времени. Понятие надежности является качественным и, кроме того, допускает определение отказа. Поэтому вводятся количественные характеристики надежности, которые могут быть указаны в техническом задании или в руководящих документах (вероятность безотказной работы, интенсивность отказов, коэффициент готовности и т.д.). Эти количественные характеристики позволяют применить математические методы оценки величин на основе теории вероятностей и математической статистики для определения достигнутого уровня надежности, так как характеристики надежности главным образом зависят от числа отказов в единицу времени. Расчет показателей надежности является общепринятой практикой и входит ГОСТ по проектированию систем управления [1]. Примером такого расчета может служить работа Кузнецовой Н.И. [2].

Поскольку в АСУ ТП присутствует программное обеспечение (является составным элементом АСУ ТП), то отказ программных изделий может вызвать потерю возможности выполнения требуемой функции. Чаще всего, выявить ошибки в ПО и определить надежность продукта можно выявить только на этапах тестирования и эксплуатации, однако сделать прогноз частоты появления ошибок возможно и на стадии проектирования. Более подробное описание моделей надежности программного обеспечения и расчет надежности ПО представлены в работе Бойковой [3].

ИСТОЧНИКИ ОТКАЗОВ ПРОГРАММНЫХ СРЕДСТВ И ИХ ПРЕДУПРЕЖДЕНИЕ

Можно выделить следующие основные источники отказов программных средств:

1) несовершенство технического задания;

2) ошибки при программировании;

3) неправильная эксплуатация/изменение условий эксплуатации.

Данные категории тесно связаны с человеком и возникают, в большинстве случаев, как следствие его деятельности.

Этап составления технического задания на программирование охватывает, в основном, принципиальную алгоритмическую часть. Вместе с тем, имеется достаточно большое количество вопросов, на которые следовало бы обращать внимание при составлении ТЗ. Неправильное формирование ТЗ на разработку программного обеспечения часто приводит к последующему выходу из строя ПО и отказу оборудования и/или системы управления в целом. Зачастую, ошибки на этапе составления ТЗ являются самыми критичными и трудно прогнозируемыми, поскольку выявление ошибок на последующих этапах жизненного цикла изделия поддаются программно-аппаратной диагностике. Также, при проектировании необходимо учитывать множество сторонних факторов, влияющих на безопасность и надежность

эксплуатации. Удобство интерфейса пользователя, своевременное оповещение о возможных ошибках и выходе из строя – необходимо продумывать уже на этапе формирования ТЗ, так как пренебрежение данным функционалом непременно приведет к ошибкам в эксплуатации.

Ошибка программирования – это, прежде всего, неверное исполнение программистом требований технического задания. Наиболее часто такие ошибки возникают при программировании сложных вычислительных алгоритмов, в которых имеется большое количество условий. Здесь могут быть ошибки при организации циклов (особенно вложенных), ошибки при выполнении логических переходов, не точная классификация переменных (например, в определении глобальных переменных) и т.д.

Для устранения или уменьшения числа ошибок рекомендуется модульное исполнение программного обеспечения. Модули не должны содержать большое число операторов. Известной реализацией этого подхода является создание библиотек стандартных подпрограмм. В своей работе, Jung-Hua [4] продемонстрировал оценки надежности модульного программного обеспечения с учетом различных комбинаций входов и выходов системы, а также анализ робастности компонентов. Помимо модульного исполнения, в настоящий момент существуют программные проверки исходного кода на предмет синтаксических и логических ошибок. Одной из таких программ является SonarQube. Также, на предприятиях и проектах активно внедряется система контроля качества производства по европейским стандартам ISO 9001 и стандарты Quality Assurance.

Отказы, возникающие в следствие эксплуатации, следует рассматривать с единой позиции: отказов функций управления всей системы (АСУ ТП). Внешне может показаться, что отказ функций происходит по вине ПО, поскольку эксплуатационный персонал, в итоге, получает информацию от работы ПО. Однако истинные источники отказов могут быть иными, часто не связанными со свойствами программ.

Этот вид отказов может вызываться целым рядом причин:

– отказы технических средств, ресурсы которых использует программа (меняются условия работы ПО);

– изменение градуировочных характеристик первичных датчиков, с помощью которых ведется измерение важных физических величин (например, при изменении физических условий работы датчиков, когда, в частности, показания датчиков температуры подвергаются искажению из-за охлаждения по внешним причинам, метрологические характеристики данных становятся неприемлемыми);

– неуверенные действия пользователя, который не имеет достаточных навыков работы с эксплуатационной документацией (появился новый работник, не имеющий должного опыта работы, фактически это изменение условий эксплуатации);

– изменение климатических условий работы технических средств, когда нарушаются допустимые пределы температуры, окружающей среды, или уровень электромагнитных помех становится недопустимо большим и т.д.

Все причины отказов программного обеспечения, возникающих при изменении условий эксплуатации, вряд ли можно назвать на стадии проектирования систем. Тем не менее, имеются определенные средства, позволяющие учесть этот неблагоприятный фактор. К таким средствам можно отнести:

– предварительное обучение эксплуатационного персонала;

– контроль результатов измерения физических величин на принадлежность реальному диапазону значений;

– использование специальных алгоритмов обнаружения неисправных датчиков;

– проведение профилактических работ с целью поддержания работоспособности технических средств и т.д.

Поскольку АСУ ТП является сложной системой и предполагается, что она обслуживается и используется рядом эксплуатационных подразделений. Поэтому, можно ожидать отказы в работе программных средств от неправильных действий персонала. Данный вопрос касается не только своевременного и правильного обслуживания АСУ ТП персоналом, но и, например, действий операторов в пультовых. Современные системы управления обладают высокой стоимостью, поэтому защита от некорректных действий операторов является критически необходимым элементом. Более подробный анализ деятельности персонала АЭС и на химическом предприятии и влияние принятых решений в критических ситуациях представлено в работе Zarei [5].

Из-за специфики человеческого фактора, невозможно перечислить все механизмы отказов по причине ошибок персонала. Однако ясно, что требуется применять в первую очередь организационные меры устранения подобных отказов. Например, дублирование действий при подготовке информации, автоматическая проверка правильности информации по выбранным признакам, проверка выполнения плана профилактических работ, документирование действий с целью повышения внимания и ответственности выполнения операций эксплуатационным персоналом и т.д.

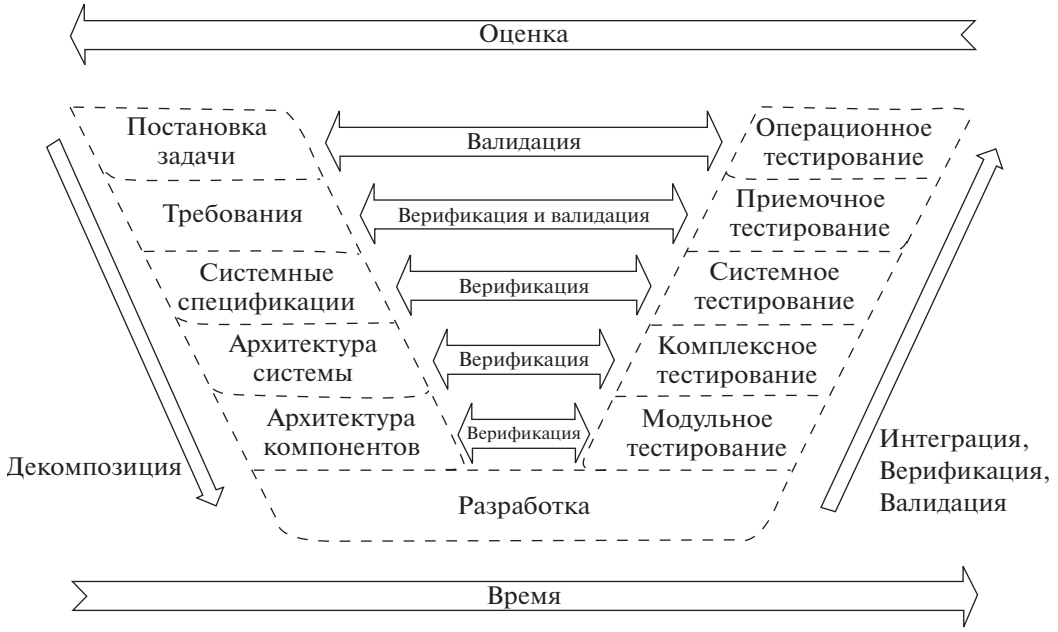

Рис. 1. V-модель жизненного цикла системы управления.

ВАЛИДАЦИЯ И ВЕРИФИКАЦИЯ

Процесс разработки программных изделий, обладающих предположительно высоким качеством, в конечном итоге приводит к созданию реального продукта. Однако, даже при выполнении всех рекомендованных мер по обеспечению качества и надежности невозможно утверждать, что требуемое качество достигнуто. Причинами этого являются не только возможные ошибки разработчика, но и сложность учета среды и всех особенностей функционирования изделия. Общей практикой является декомпозиция общей проблемы, которая приводит к рассмотрению отдельных ее фрагментов. Метод “от общего к частному” также активно используется при проектировании систем управления и ее программных компонентов [6, 7].

Верификация является неотъемлемой частью создания программного изделия, которое предполагает определение степени готовности этого изделия к эксплуатации. Верификация должна проводиться согласно утвержденной методике после предъявления разработчиком подготовленного им изделия или его части [8, 9]. Общая схема создания программного изделия или системы управления описывается в рамках V-модели, представленной на рис. 1.

При отрицательных результатах верификации программное изделие подлежит доработке.

Процедура верификации предполагает анализ всех требуемых согласно методике показателей качества. Однако, программа верификации готовится группой верификации, которая и определяет необходимый перечень показателей качества. Это связано с тем, что ряд требований к качеству ПО могут оказаться несущественными. Методика верификации ПО должна охватывать возможность выявления наиболее распространенных ошибок, встречающихся при создании программного обеспечения.

Важной частью верификации является подготовка протокола испытаний согласно утвержденной программе испытаний, где отражаются все замеченные недостатки, как по реализованным функциям, так и по качеству программной документации.

Основным назначением этапа валидации ПО является подтверждение работоспособности программной продукции в реальных условиях ее эксплуатации. Валидация проводится согласно подготовленной программе, в которой предусматривается совместное тестирование технических и программных средств. Важным требованием к валидации является испытание всего программно-технического комплекса в диапазоне всех значений сигналов, которые могут встретиться в процессе эксплуатации. При испытаниях проверяются динамические характеристики ПТК, которые должны удовлетворять требованиям, вытекающим из качества выполнения функций управления. Должны быть описаны дополнительные средства, применяемые для реализации процесса испытаний ПТК (к таким средствам относятся дополнительное оборудование, программы имитации входных сигналов, программы, с помощью которых фиксируются важные события, возникающие при испытаниях, и т.д.). Ре-

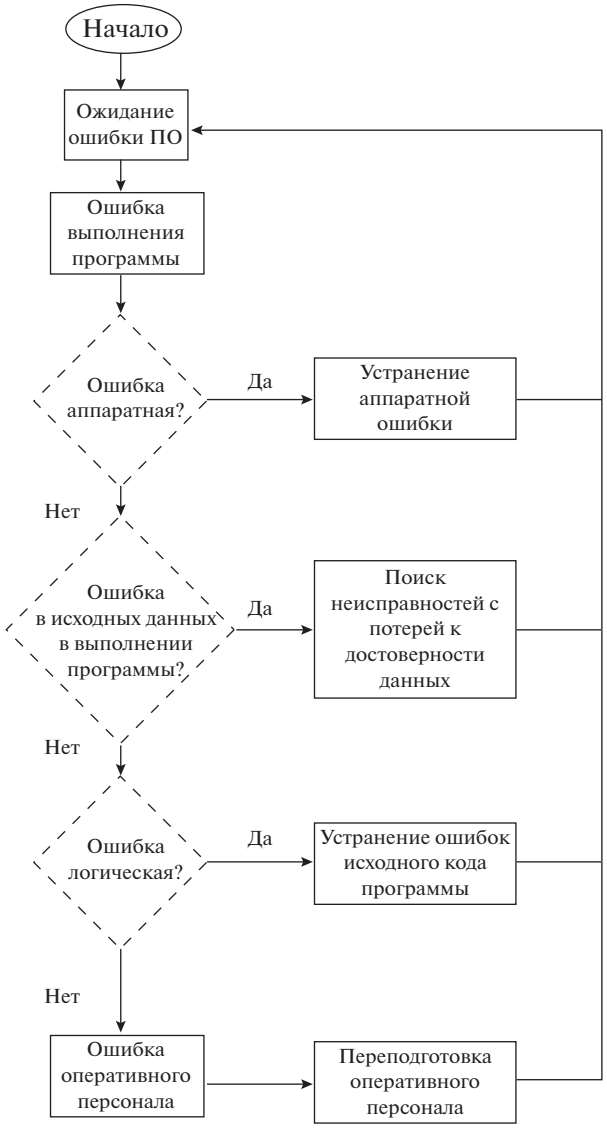

Рис. 2. Алгоритм определения характера ошибки ПО системы управления.

зультаты валидации продукта документируются и оцениваются специалистами, не участвовавшими в проектировании системы управления или программного продукта. В работе Жарко [10] показано, как на основе модели менеджмента кибербезопасности проводить валидацию и верификацию программного обеспечения для АСУТП АЭС для достижения необходимого уровня безопасности.

Несмотря на то, что на этапах верификации и валидации проводится тщательный анализ программного обеспечения и условий его работы, тем не менее опыт показывает возможность появления в процессе эксплуатации ошибок работы ПО. Это связано с тем, что на этапе проектирования невозможно учесть все причины отказов ПО. На основе анализа опыта эксплуатации различных программных изделий авторы предлагают алгоритм для определения типа возникшей ошибки, изображенный на рис. 2.

В его основе лежит последовательное отсечение возможных источников отказов и предложены меры, в том числе и организационные, которые способствовали бы улучшению надежности эксплуатации не только программного обеспечения систем управления, но и АСУ ТП в целом.

ЗАКЛЮЧЕНИЕ

Анализ литературных источников и опыта создания программного обеспечения АСУ ТП показал, что отказы ПО могут возникать по многим причинам и должны применяться меры по их устранению на протяжении всего жизненного цикла ПО.

Основными источниками отказов ПО могут явиться:

– отсутствие постоянного внимания к обеспечению качества ПО на всех этапах его создания (следует руководствоваться программой обеспечения качества);

– недостаточно тщательная проработка алгоритмического обеспечения, на основе которого создается техническое задание на программирование (могут не учитываться диапазоны изменения данных, сложность реализации вычислительных процедур, связанных со случаями вырождения матриц и т.д.);

– игнорирование программистами известных требований к текстам программ (использование не рекомендованных программных конструкций, способов организации циклов и т.д.);

– отсутствие защиты в программах от недопустимых вычислительных операций;

– отсутствие организационных мер, предназначенных для контроля правильности подготовки информации, необходимой для работы ПО;

– недостаточная подготовка персонала, ведущего эксплуатацию ПО;

– значительные изменения условий эксплуатации, при которых могут могут возникать отказы программного обеспечения.

Поскольку алгоритм программ может оказаться непротиворечивым, но отказы ПО тем не менее могут возникать, то требуется системный подход к обеспечению надежности ПО, учитывающий влияние всех факторов, приводящих к возможности появления отказа ПО.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34.201-89.
2. *Кузнецова Н.И., Баканов Д.В.* Оценка надежности систем диагностирования АСУ ТП АЭС и методы

ее повышения // Энергетические установки и технологии. 2020. Т. 6. № 1. С. 46–52.

3. *Бойкова О.Г., Чистякова Т.Б., Бокий Д.И.* Методика оценки надежности программно-технических комплексов АСУ ТП для электростанций малой мощности // Сборник: труды международной научно-практической конференции “передовые информационные технологии, средства и системы автоматизации, и их внедрение на российских предприятиях” aita-2011. 2011. С. 380–387.
4. *Jung-Hua Lo, Chin-Yu Huang, Ing-Yi Chen, Sy-Yen Kuo, Lyu Michael R.* Reliability assessment and sensitivity analysis of software reliability growth modeling based on software module structure // The Journal of Systems and Software. 2005. V. 76. P. 3–13.
5. *Zarei E., Khan F., Abbassi R.* Importance of human reliability in process operation: A critical analysis // Reliability Engineering & System Safety. 2021. V. 211. P. 107607. https://doi.org/10.1016/j.ress.2021.107607
6. *Кузнецов П.А., Ковалев И.В.* Надежность АСУ ТП с учетом ее функциональности // Актуальные проблемы авиации и космонавтики. 2014. Т. 1. № 10. С. 316–317.
7. *Аракелян Э.К., Саркисян Р.Е., Мезин С.В.* Оптимизация характеристик надежности АСУ ТП, основанная на концепции анализа иерархий // Теплоэнергетика. 2001. № 10. С. 7–12.
8. *Власов В.А., Толоконский А.О., Беседин Г.А., Симашин А.Н.* Верификация ПО для замкнутых систем управления // Ядерные измерительно-информационные технологии. 2009. № 2. С. 101–103.
9. *Власов В.А., Толоконский А.О., Голованев В.Е.* Анализ вероятности отказа систем отображения // Промышленные АСУ и контроллеры. 2005. № 4. С. 25–28.
10. *Jharko E.* Systems Important for NPP Safety: Software Verification and Cybersecurity. In: *Radionov A.A., Gasiyarov V.R.* (eds.) Advances in Automation II. RusAutoCon 2020 // Lecture Notes in Electrical Engineering. 2021. V. 729. Springer, Cham. https://doi.org/10.1007/978-3-030-71119-1_10

Vestnik Nacional’nogo Issledovatel’skogo Yadernogo Universiteta “MIFI”, 2021, vol. 10, no. 5, pp. 429–435

Basic Aspects of the Reliability of Control System Software

A. A. Zvonareva[a,#] and A. O. Tolokonskiy[a,##]

[a] *National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, 115409 Russia*

[#] *e-mail: AAZvonareva@mephi.ru*

[##] *e-mail: toloconne@yandex.ru*

Received December 20, 2021; revised December 21, 2021; accepted December 30, 2021

Abstract—Reliability is one of the most important quality parameters. Since the software is an integral part of the process control system, the failure of software components causes a serious decrease in the product reliability and can cause the loss of the required function. The main sources of control system software and hardware failures in the nuclear industry are described and methods for preventing malfunctions are considered. Nevertheless, experience in software development allows us to highlight the most common errors in its design. The consolidated reasons for software failures include imperfection of the technical task for programming, errors of the programmer developing software modules, errors of operating personnel using software, changes in software operating conditions, the possibility of the appearance of unacceptable arithmetic operations, and an insufficiently complete analysis of the properties of the system in which the software is functioning. Errors made during programming cannot always be quickly noticed when analyzing the text of a program module. This is especially true of program modules having complex logical operations. Therefore, during verification, one should be guided by the documents intended to ensure the quality of the program module, which contain recommendations for usage typical software designs, sizes of software modules, etc.

Keywords: reliability, failure, reason, software, validation, verification

DOI: 10.1134/S2304487X21050126

REFERENCES

1. GOST 34.201-89.
2. Kuznetsova N.I., Bakanov D.V., Ocenka nadezhnosti sistem diagnostirovaniya ASU TP AES i metody eyo povysheniya [Evaluation of reliability of npp apcs diagnostics systems and methods of its enhancemen], *Energeticheskiye ustanovki i tekhnologii,* 2020, vol. 6, no. 1, pp. 46–52 (in Russian).
3. Boykova O.G., Chistyakova T.B., Bokiy D.I., Metodika otsenki nadezhnosti programmno-tekhnicheskikh

kompleksov ASU TP dlya elektrostantsiy maloy moshchnosti, *V sbornike: trudy mezhdunarodnoy nauchno-prakticheskoy konferentsii "peredovyye informatsionnyye tekhnologii, sredstva i sistemy avtomatizatsii, i ikh vnedreniye na rossiyskikh predpriyatiyakh" aita-2011*, 2011, pp. 380–387 (in Russian).

4. Jung-Hua Lo, Chin-Yu Huang, Ing-Yi Chen, Sy-Yen Kuo, Lyu M. R., Reliability assessment and sensitivity analysis of software reliability growth modeling based on software module structure, *The Journal of Systems and Software*, 2005, vol. 76, pp. 3–13.
5. Zarei E., Khan F., and Abbassi, R., Importance of human reliability in process operation: A critical analysis, *Reliability Engineering & System Safety*, 2021, vol. 211, 107607.
https://doi.org/10.1016/j.ress.2021.107607
6. Kuznetsov P.A., Kovalev I.V., Nadezhnost' ASU TP s uchetom yeye funktsional'nosti [Reliability of the automated control system taking into account its functionality], *Aktual'nyye problemy aviatsii i kosmonavtiki,* 2014, vol. 1, no. 10, pp. 316–317 (in Russian).
7. Arakelyan E.K., Sarkisyan R.Ye., Mezin S.V., Optimizatsiya kharakteristik nadezhnosti ASU TP, osnovannaya na kontseptsii analiza iyerarkhiy, *Teploenergetika*, 2001, no. 10, pp. 7–12 (in Russian).
8. Vlasov V.A., Tolokonskiy A.O., Besedin G.A., Simashin A.N., Verifikatsiya po dlya zamnutykh sistem upravleniya [Software verification for closed control system] *Yadernyye izmeritel'no-informatsionnyye tekhnologii*, 2009, no. 2, pp. 101–103 (in Russian).
9. Vlasov V.A., Tolokonskiy A.O., and Golovanev V.Ye., Analiz veroyatnosti otkaza sistem otobrazheniya [Analysis of the probability of failure of display systems], *Promyshlennyye ASU i kontrollery*, 2005, no. 4, pp. 25–28 (in Russian).
10. Jharko E., Systems Important for NPP Safety: Software Verification and Cybersecurity, In: Radionov A.A., Gasiyarov V.R., Eds., Advances in Automation II. RusAutoCon 2020, *Lecture Notes in Electrical Engineering*, 2021, vol. 729, Springer, Cham.
https://doi.org/10.1007/978-3-030-71119-1_10