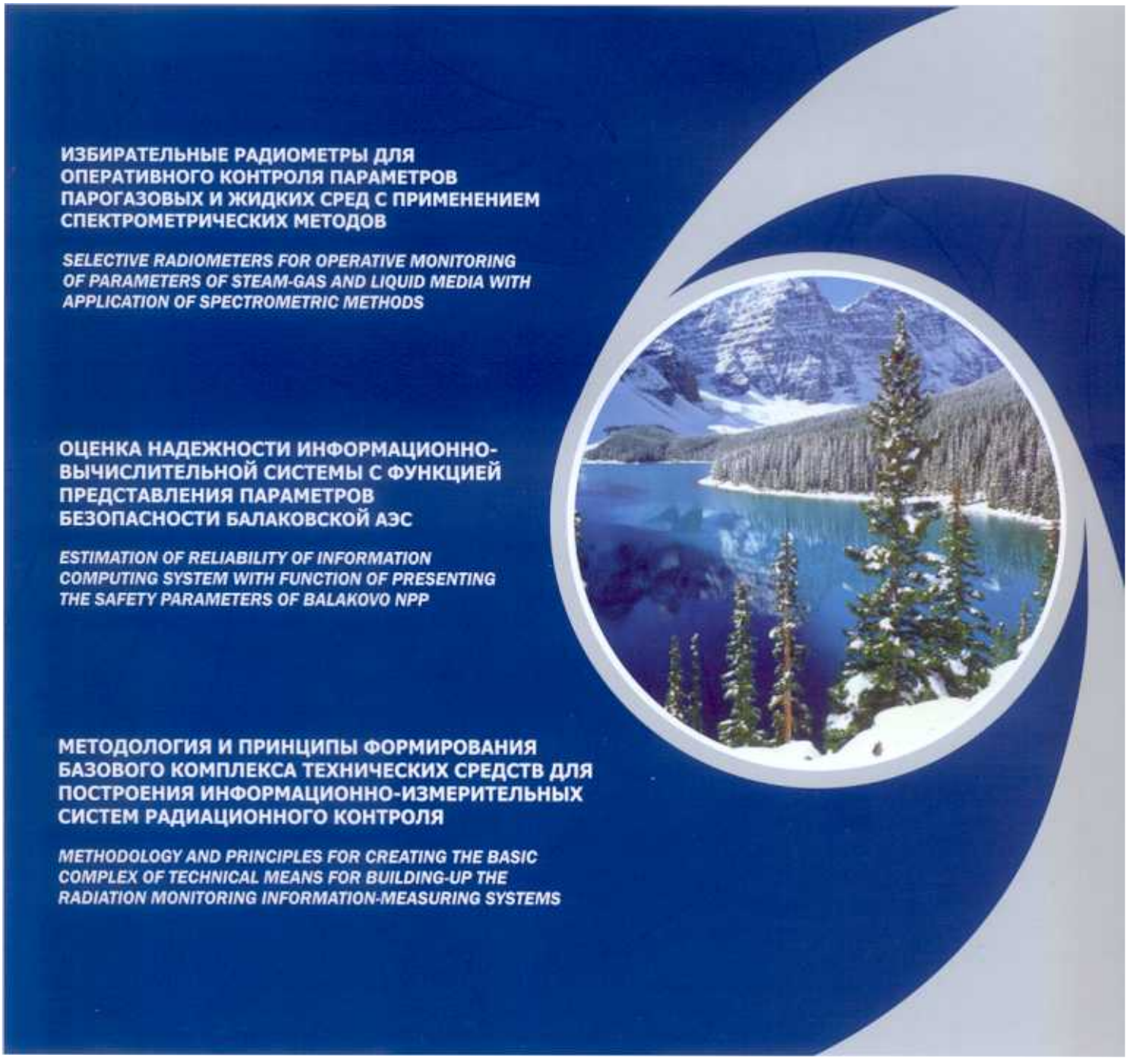
4 (20)
2006

ЯДЕРНЫЕ ИЗМЕРИТЕЛЬНО-ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

NUCLEAR MEASUREMENT & INFORMATION TECHNOLOGIES



A journal of IEC/TC45 «Nuclear Instrumentation»
Журнал МЭК/ТК45 «Ядерное приборостроение»

Токмачев Г.В., Подколзина Л.В., Лобанок О.И.

ОЦЕНКА НАДЕЖНОСТИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ С ФУНКЦИЕЙ ПРЕДСТАВЛЕНИЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ БАЛАКОВСКОЙ АЭС

В статье описаны методика и результаты анализа надежности информационно-вычислительной системы с функцией представления параметров безопасности, внедряемой на 1-м энергоблоке Балаковской атомной станции в рамках программы ТАСИС. Обсуждены вопросы анализа надежности персонала, оценки отказов по общей причине, анализа надежности программного обеспечения и надежности системы в условиях обесточивания атомной станции

Tokmachev G.V., Podkolzina L.V., Lobanok O.I.

ESTIMATION OF RELIABILITY OF INFORMATION COMPUTING SYSTEM WITH FUNCTION OF PRESENTING THE SAFETY PARAMETERS OF BALAKOVO NPP

In the paper the procedure and the results of analysis of the reliability of information computing system with the function of presenting the safety parameters being implemented at Balakovo NPP Unit 1 in the framework of realizing TACIS program are described. The problems of analysis of the personnel's reliability, estimation of the common mode failures, analysis of the reliability of the software and the reliability of the system in conditions of the NPP de-energizing are discussed.

1. ВВЕДЕНИЕ

В рамках программы ТАСИС на 1-м энергоблоке Балаковской АЭС внедряется информационно-вычислительная система с функцией представления параметров безопасности (ИВС/СППБ), которая является полностью интегрированной микропроцессорной системой реального времени и предназначена для сбора, отображения и регистрации аналоговых, дискретных и расчетных параметров и трендов. В статье представлены результаты анализа надежности этой системы.

Работа выполнена в соответствии с требованиями ОПБ-88/97 [1] и НП-026-01 [2], которые предписывают, чтобы проект управляющих систем, важных для безопасности, содержал:

- анализ реакции систем управления и контроля реакторной установки и энергоблока АЭС на возможные отказы в системе;
- и анализ надежности функционирования технических и программных средств и системы в целом с учетом отказов по общей причине и ошибок персонала.

2. ХАРАКТЕРИСТИКА МОДЕЛИРУЕМОЙ СИСТЕМЫ

Надежность ИВС/СППБ определяется исходя из выполняемых функций и влияния этих

1. INTRODUCTION

In the framework of realizing TACIS program the information computing system with the function of presenting the safety parameters (ICS/SPPS) is being implemented at Balakovo NPP Unit 1. This system is a fully integrated real time microprocessor system and is intended for acquisition, displaying and registration of analog, discrete and calculated parameters and trends. In the paper the results of the analysis of this system reliability are demonstrated.

The work has been performed in accordance with the requirements of OPB-88/97 [1] and NP-026-01 [2], which formulated the necessity of availability of the following analyses for the project of control systems important to safety:

- analysis of response of the instrumentation and control systems of the reactor plant and NPP power Unit to possible failures in the system and;
- analysis of reliability of functioning of the technical and program means and the system as a whole with regard for the common mode failures and error of the personnel.

2. CHARACTERISTIC OF MODULATED SYSTEM

The reliability of ICS/SPPS is determined on the basis of the functions executed and of

функций на безопасность и надежность энергоблока (выработку электроэнергии). Все функции, выполняемые ИВС/СППБ, можно объединить в следующие пакеты:

- поддержание конфигурации и функционирования ИВС/СППБ;
- сбор и первичная обработка информации;
- расчеты;
- архивирование и хранение информации;
- сигнализация об отклонениях в работе энергоблока, изменениях состояния оборудования и выходе параметров энергоблока за установленные проектом границы;
- работа с процедурами и документами;
- представление информации.

Конечной функцией ИВС/СППБ, требующей выполнения всех других функций, является представление оперативному персоналу энергоблока (ведущим инженерам управления реактором и турбиной, а также начальнику смены блока) информации, необходимой для автоматизированного управления, с целью предотвращения нарушения пределов безопасной эксплуатации или уменьшения последствий аварии. Надежность по функции представления информации является для ИВС/СППБ интегральным показателем.

В рамках проведенного анализа критерием отказа ИВС/СППБ является отсутствие информации на всех мониторах хотя бы одного из рабочих мест блочного или резервного щита управления (БЩУ или РЩУ):

- рабочего места ведущего инженера управления реактором (ВИУР) на БЩУ;
- рабочего места ведущего инженера управления турбиной (ВИУТ) на БЩУ;
- рабочего места начальника смены блока (НСБ) на БЩУ;
- панелей расхолаживания РЩУ.

Анализ надежности ИВС/СППБ выполнен для критических элементов и подсистем, необходимых для поддержания работоспособности ИВС/СППБ. ИВС/СППБ относится к восстанавливаемым и обслуживаемым системам длительного применения. Режим работы ИВС/СППБ – непрерывный. Система должна обеспечивать возможность восстановления при отказах путем замены отказавших блоков, модулей и устройств на исправные из состава ЗИП. В системе применено структурное дублирование технических средств с соответствующей программной поддержкой для решения задач переключения устройств. Процесс переключения с рабочего модуля на резервный происходит без нарушения процесса выполнения функций другими элементами системы, а также не накладывает временные и другие ограничения на работу программного обеспечения и процесс подготовки и передачи данных другим модулям системы. Принцип резервирования потоков данных показан на примере взаимодействия альфа-серверов и устройств рабочего места ВИУР на рис. 1.

the influence of these functions on the safety and reliability of the power Unit (on generation of electric energy). All the functions executed by ICS/SPPS could be combined into the following packages:

- support of configuration and functioning of ICS/SPPS;
- acquisition and primary processing of information;
- calculations;
- archiving and storage of information;
- signaling on deviations in the operation of the power Unit, on changes of state of the equipment and deviation of the power Unit parameters from the boundaries established by the project;
- work with procedures and documents;
- presentation of information.

The final function of ICS/SPPS, requiring the fulfillment of all other functions, is the presentation to the shift personnel of the power Unit (to Leading engineers of reactor and turbine control and to the Chief of shift of Unit) of the information required for the automated control in order to prevent the disturbances of the safe operation limits or to decrease the consequences of an accident. The reliability by function of presenting the information is the integral factor for ICS/SPPS.

In the framework of the analysis fulfilled the criterion of ICS/SPPS failure is the absence of information at all monitors of at least one working place in Main control room or Emergency control room (MCR or ECR):

- working place of Leading engineer of reactor control (LERC) in MCR;
- working place of Leading engineer of turbine control (LETC) in MCR;
- working place of the Chief of shift of Unit (CSU) in MCR;
- cooling panels in ECR.

The analysis of ICS/SPPS reliability has been fulfilled for critical elements and subsystems required for supporting the operability of ICS/SPPS. ICS/SPPS is related to recovered and maintained systems of durable application. The operation mode of ICS/SPPS is continuous. The system shall ensure the possibility of recovery at failures by replacement of the failed units, modules and devices for properly functioning ones taken from the set of Spare Parts. In the system the structural redundancy of the technical means is applied with relevant program support for solving the tasks of the devices switching over. The process of switching over from working module to the redundant one is carried out without disturbance of the process of executing the functions by other elements of the system and does not cause time and other limitations on operation of the software and on preparation and transfer of the data to other modules of the system. The principle of redundancy of the data flows is shown in Figure 1 for inter-

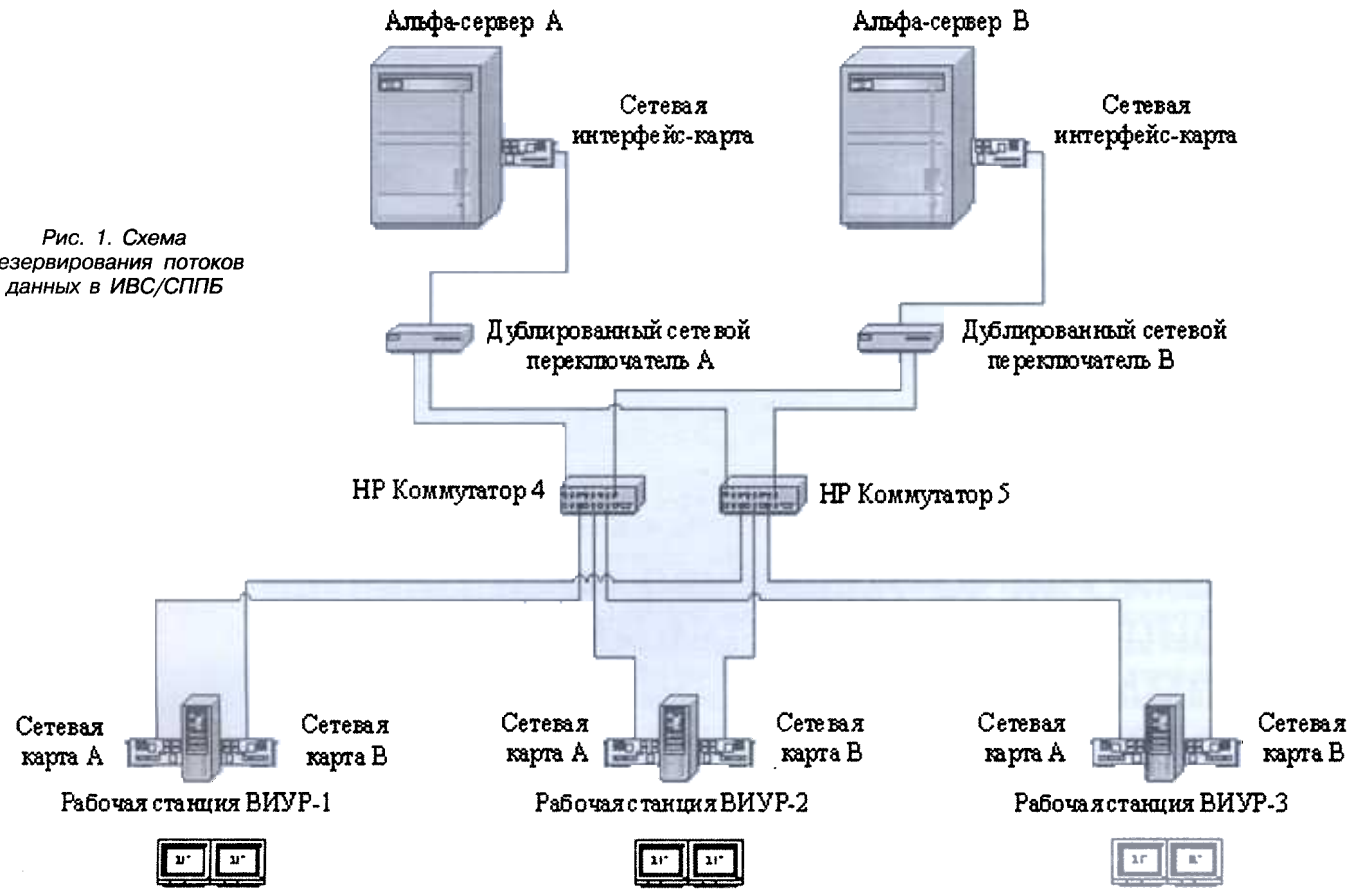


Рис. 1. Схема резервирования потоков данных в ИВС/СППБ

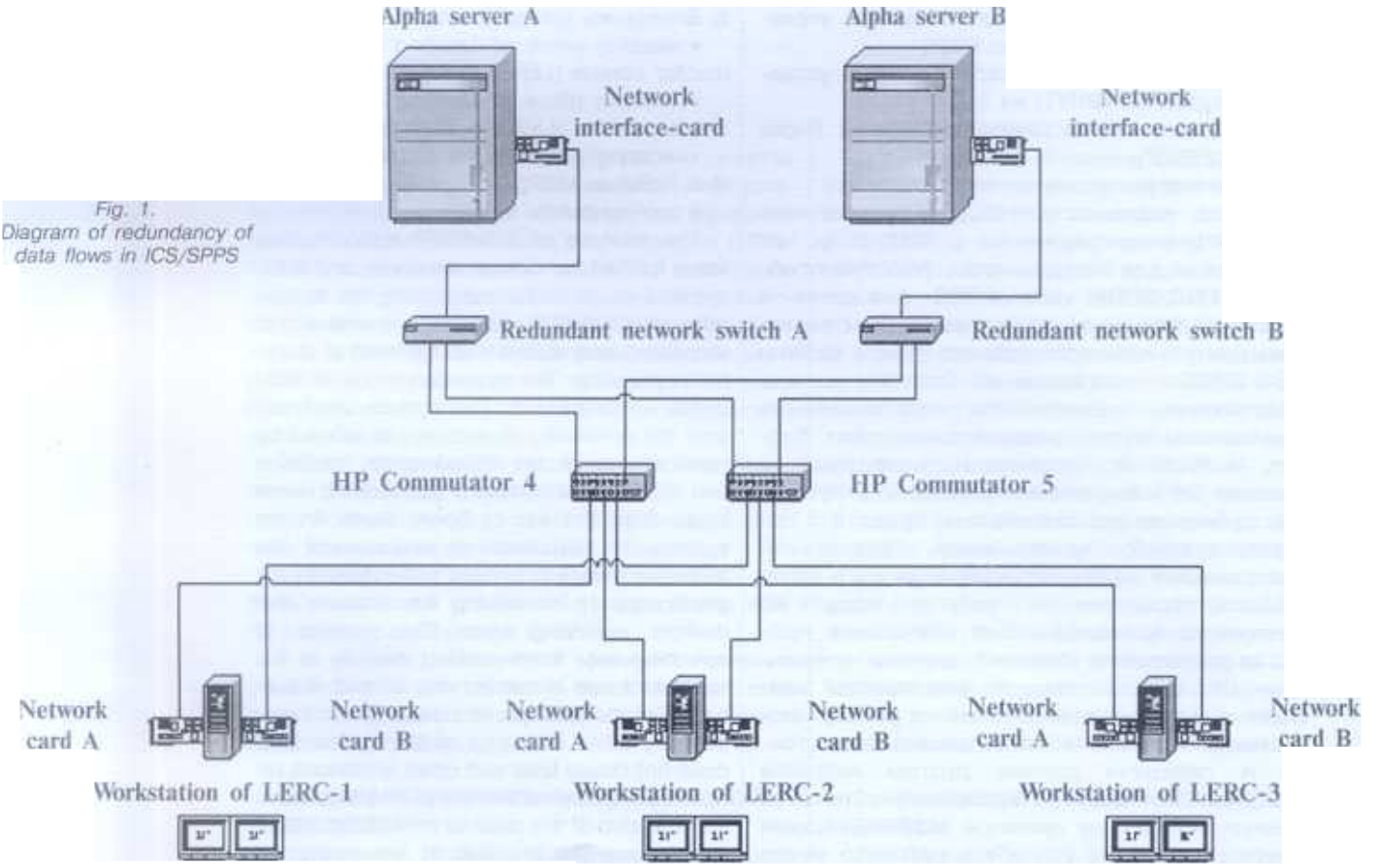


Fig. 1. Diagram of redundancy of data flows in ICS/SPPS

В системе также применено временное резервирование за счет использования источников бесперебойного питания, которые наряду с аккумуляторными батареями АЭС обеспечивают резерв времени для обнаружения и устранения отказов.

Для защиты целостности данных, хранящихся на альфа-серверах, используются несколько дисков, объединенных в единый массив. Обеспечение отказоустойчивости альфа-сервера в системе осуществляется путем зеркального отображения дисков, т.е. одна и та же информация одновременно записывается на два различных диска, использующих один контроллер. Если один диск или его раздел отказывает, то для продолжения работы системы используется зеркальный диск.

В системе внедрены внутренний автоматический контроль и идентификация отказов. Система имеет визуальный индикатор отказа аппаратных средств, который всегда является видимым (независимо от того, какой монитор работает) и меняет цветовую индикацию с зеленой на красную, если контролируемый элемент системы выходит из строя.

3. МЕТОДИКА АНАЛИЗА НАДЕЖНОСТИ СИСТЕМЫ

Анализ надежности проводится на основе метода дерева отказов, который предусматривает формирование логического условия неработоспособности анализируемой структуры в форме дерева отказов, генерацию минимальных сечений и расчет показателей неготовности указанных сечений и структуры в целом. Метод широко используется в мировой практике и подробно описан в литературе [3]. Применительно к системам управления методология апробирована при выполнении анализов надежности АСУ ТП в рамках разработки новых проектов, в частности, для АЭС Нововоронежская-2 [4].

Для разработки модели и проведения расчета надежности системы использована программа RISK SPECTRUM PSA Professional, которая аттестована Российским надзорным органом и применяется для выполнения как анализа надежности систем произвольной структуры, так и для проведения полномасштабного ВАБ уровня 1 методом деревьев событий и/или деревьев отказов [5]. Основу алгоритма расчетов составляют генерация и количественный расчет вероятности реализации минимальных сечений, представляющих собой минимальный по количеству набор событий (отказы элементов и ошибки персонала), которые обусловливают наступление вершинного события анализируемого дерева отказов (неготовность системы). При этом RISK SPECTRUM PSA Professional позволяет неявно моделировать отказы по общим причинам на деревьях отказов.

В рамках настоящей работы выполнен качественный и количественный анализ надежности системы. При проведении качественного анализа определены виды и последствия отказов технических и программных средств, которые могут привести к отказу системы.

face of alpha servers and devices of working place of LERC.

He system the time reserve is also applied die to the use of the uninterruptible supply sources, which together with the accumulator batteries of NPP provide the time reserve for revealing and eliminating the failures.

For protecting the integrity of the data stored at alpha servers several disks combined into one array are used. The provision of fault tolerance of alpha server in the system is performed by mirror presentation of disks, i.e. one and the same information is recorded simultaneously at two different disks, which use one controller. If one disk or its part is failed, the mirror disk is used for continuation of operation of the system.

In the system the internal automatic check and identification of failures are implemented. The system has visual indicator of failure of the hardware, which is always visible (independently of what monitor is operated), and the color indication is changed from green to red, if the checked element of the system is failed.

3. PROCEDURE FOR ANALYSIS OF RELIABILITY OF THE SYSTEM

The analysis of the reliability is fulfilled on the basis of the method of the tree of faults, which envisages the generation of logical condition of non-operability of the analyzed structure in the form of tree of faults, generation of minimum sections and calculation of unavailability factors of the specified sections and the structure as a whole. The method is widely applied in the world practice and is described in details in paper [3]. Applicably to the control systems the methodology has been approved during fulfillment of analyses of the APCS reliability within the framework of developing new projects, in particular, for Novo-Voronezh NPP-2 [4].

For developing the model and for conducting the calculation of the reliability of the system the program RISK SPECTRUM PSA Professional has been used. This program is certified by the Russian supervisory organization and is applied for fulfilling the analysis of the reliability of systems having arbitrary structure and for conducting full-scale probabilistic analysis of safety PAS of level 1 by the method of trees of events and/or trees of faults as well [5]. The basis of algorithm of the calculations deals with generation and quantitative calculation of probability of realizing minimum sections, presenting minimum by amount set of events (failures of elements and errors of personnel), which cause the occurrence of the top event of the analyzed tree of faults (unavailability of the system). At this RISK SPECTRUM PSA Professional permits to simulate implicitly the common mode failures at trees of faults.

Within the framework of this work the qualitative and quantitative analysis of the system reli-

гут повлиять на выполнение системой заданных функций, и разработана вероятностная модель, определяющая условие отказа анализируемой структуры ИВС/СППБ.

При разработке вероятностной модели ИВС/СППБ проведена классификация первичных событий по видам контроля отказов и возможности восстановления отказавших элементов.

Так как система установлена в помещении с постоянным пребыванием персонала, то отказы, идентифицируемые сразу или в течение короткого времени после их возникновения при помощи встроенных элементов внутренней диагностики, являются постоянно контролируемыми. Исключением являются переключатели резервного питания, отказы которых проявляются при возникновении требования на срабатывание или при проведении периодических проверок прохождения сигнала. Эти элементы моделировались как периодически контролируемые. Также отнесены к периодически контролируемым источники бесперебойного питания и их зарядные устройства, эффективность работы которых в режиме разряда и заряда, соответственно, не может контролироваться в условиях электроснабжения от внешнего источника.

Мониторы БЩУ, которые не имеют внутренней системы диагностики, являются непрерывно контролируемыми устройствами, так как их отказ (потеря изображения) немедленно обнаруживается оператором. В то же время мониторы РЩУ отнесены к периодически контролируемым элементам системы. Предполагается, что их отказы будут выявляться при периодических обходах специалистами цеха тепловой автоматики и измерений (ТАИ).

Анализ показал, что все элементы системы являются восстанавливаемыми. Восстановление производится путем их замены сменным персоналом цеха ТАИ. Необходимое количество ЗИП, размещенного в районе установки системы, должно быть предусмотрено на АЭС.

В результате количественного анализа выполнена оценка коэффициента неготовности системы ИВС/СППБ, для чего использованы данные по показателям надежности элементов, которые были определены разработчиком системы на основании анализа гарантийных сроков, установленных фирмами-производителями оборудования системы.

Ниже охарактеризованы специальные задачи, решенные в рамках анализа надежности системы.

4. АНАЛИЗ ОШИБОК ПЕРСОНАЛА

При проведении анализа рассмотрены только те действия (и соответственно, ошибки) персонала, которые допускаются при выполнении им поставленных задач. Злоумышленные действия, т.е. преднамеренные диверсионные действия или акты саботажа и т.п., не являются предметом анализа надежности персонала.

Технические решения, реализованные в проекте ИВС/СППБ, значительно уменьшают число возможных ошибочных действий персонала:

ability has been fulfilled. During fulfillment of the qualitative analysis the types and consequences of faults of the technical and program means, which could have influence on executing the specified functions by the system, have been determined, and the probabilistic model determining the condition of failure of the analyzed structure of ICS/SPPS has been developed.

During the development of the probabilistic model of ICS/SPPS the classification of the primary events by types of check of the faults and the possibility of recovering the failed elements have been fulfilled.

As the system is installed in room with permanent staying of the personnel, the faults identified just after or during short period of time after their occurrence by means of built-in elements of internal diagnostics, are permanently monitored. Exception is made for switches of redundant supply, which failures are manifested at occurrence of the request for actuation or during execution of periodic checks of the signal passing. These elements have been simulated as periodically monitored. The uninterruptible supply sources and their chargers are also related to periodically monitored elements, as the efficiency of their operation in mode of discharge and charging, respectively, could not be checked in conditions of supplying from external source.

The monitors in MCR, not having internal system of diagnostics, are permanently monitored devices, as their failure (loss of image) is immediately revealed by operator. At the same time the monitors in ECR are related to periodically monitored elements of the system. It is assumed that their failures would be revealed during periodical inspections performed by specialists of thermal automatics and measurements shop (TAM).

The analysis has demonstrated that all the elements of the system are recoverable. The recovery is fulfilled by their replacement executed by the shift personnel of the TAM shop. The necessary amount of Spare Parts shall be envisaged at NPP and the Spare Parts shall be located in the area of the system installation.

In the result of the quantitative analysis the estimation of the unavailability coefficient of the ICS/SPPS system has been performed, for this purpose the data on reliability factors of the elements, determined by the system developer on the basis of analysis of the warranty periods specified by the firms-producers of the system equipment, has been used.

Below the special tasks solved with the framework of analyzing the reliability of the system are characterized.

4. ANALYSIS OF ERRORS OF THE PERSONNEL

During fulfillment of the analysis we have considered only the actions (and relatively, the errors) of the personnel, which are permissible during their execution if the tasks

• система выполняет свои функции представления оператору параметров безопасности в автоматическом режиме, т.е. от оператора не требуется действий по управлению работой системы. При этом ошибки оператора при считывании и интерпретации информации находятся за рамками настоящего анализа;

• в ИВС/СППБ информация о параметрах, важных для безопасности, защищена от несанкционированного доступа к техническим и программным средствам во время эксплуатации, поэтому ошибки оператора при оценке ситуации или при планировании действий, приводящие к выполнению неправильных действий и искажению информации, исключены;

• профилактическое обслуживание системы проходит без нарушения ее работоспособности, т.е. проведение профилактического обслуживания не требует вывода элементов системы из режима, в котором они выполняют предписанные функции.

Ошибки персонала возможны при проведении восстановления отказавших элементов путем их замены. Наиболее вероятной является ошибка при замене отказавшего диска в RAID массиве дисков переменных данных или системных дисков, когда инженер, обслуживающий систему, ошибочно меняет работоспособный диск вместо отказавшего. В этом случае замененный диск продолжает выполнять требуемые функции, а отказавший диск остается в отказовом состоянии. Следует отметить, что вероятность такой ошибки достаточно мала, так как это рутинная операция, основанная на навыках. Кроме того, напротив отказавшего диска горит сигнальная лампочка, которая продолжает гореть в случае выполнения ошибочной замены. Эта операция контролируется сменным персоналом и системой диагностики системы. Поэтому совершенная ошибка будет немедленно выявляться и ее вероятность пренебрежимо мала.

5. АНАЛИЗ ОТКАЗОВ ПО ОБЩЕЙ ПРИЧИНЕ

В настоящее время при проведении анализов надежности систем АЭС общепризнанным является подход, при котором для резервируемых элементов допускается возможность наступления множественных зависимых отказов по одной общей причине. Эта общая причина может быть связана с наличием зависимостей, не учитываемых в модели в явной форме и вызванных конструктивными, производственными и эксплуатационными факторами, которые проявляются при общем расположении, одинаковых условиях эксплуатации, применении общих процедур технического обслуживания и/или одинаковых конструкционных типах резервируемых элементов. Наличие таких факторов «общности» может привести к значительному повышению вероятности множественных отказов.

Учитывая то, что резервируемые элементы системы ИВС/СППБ расположены в одной зоне

specified. The ill-intentioned actions, i.e. premeditated diversion actions or acts of sabotage, etc., are not the subject of analysis of the personnel's reliability.

The technical solutions, realized in the project of ICS/SPPS, decrease significantly the number of possible erroneous actions of the personnel:

• The system executes its functions of presenting the safety parameters to operator in automated mode, i.e. no actions on the system operation control is required from operator. At this the errors of operator during readout and interpretation of the information are outside the framework of this analysis.

• In ICS/SPPS the information on parameters important to safety is protected from unauthorized access to technical and program means during operation, thus the errors of operator during estimation of situation or at planning the actions, leading to fulfillment of incorrect actions and distortion of information, are eliminated.

• The preventive maintenance of the system is carried out without disturbance of its operability, i.e. the execution of the preventive maintenance does not require the output of the system elements from the mode, in which they fulfill the functions specified.

The errors of the personnel are possible during fulfillment of recovery of the failed elements by their replacement. The most probable error during the replacement of failed disk in RAID massive of variable data disks or of system disks occurs when the engineer performing the maintenance of the system changes erroneously the operable disk instead of the failed one. In this case the replaced disk continues the execution of the required functions, and the failed disk is kept in the failed state. It should be noted that the probability of such an error is sufficiently low as it is a routine operation based on skills gained. Besides, the signal lamp opposite the failed disk is lighted and is continued to light in case of fulfillment of the erroneous replacement. This operation is checked by the shift personnel and by diagnostic system of the system. Thus, the error made will be revealed immediately, and its probability is negligibly low.

5. ANALYSIS OF COMMON MODE FAILURES

At present during fulfillment of analyses of the NPP systems' reliability the conventional approach is such that for redundant elements the possibility of occurrence of multiple dependent failures by common cause is permissible. This common cause could be connected with availability of relations not taken into account in the model in explicit form and caused by design, industrial and operational factors, which manifest at common location, similar conditions of operation, at application of common procedures of the technical maintenance and/or similar struc-

(помещение БЩУ, РЩУ или ИВС), важным источником возникновения отказов по общей причине могут являться внешние воздействующие факторы, такие, как влажностно-тепловые и ударно-вибрационные [6]. Оборудование системы поставляется в пожаростойком и сейсмостойком исполнении, а на БЩУ и РЩУ постоянно работают системы кондиционирования воздуха. Поэтому предполагается, что воздействие вышеуказанных факторов на элементы системы будет минимальным. Однако практика показывает, что полностью исключить отказы по общей причине невозможно.

Обычно в моделях надежности учитываются только те отказы по общей причине, которые проявляются одновременно или в короткие промежутки времени, не превосходящие по длительности характерные периоды времени, определяемые моделью надежности (среднее время восстановления для явных отказов и период испытаний для скрытых отказов в режиме ожидания). Это наиболее актуально для программируемых систем управления и контроля, для которых с высокой степенью периодичности (т.е. практически непрерывно) предусматривается внутренняя диагностика отдельных устройств и перекрестный контроль резервируемых элементов.

Отечественные нормативные документы по практическому учету отказов по общей причине программируемых систем отсутствуют. В стандарте МЭК [7], который на сегодня является единственным международным нормативным документом в этой области, сформулированы две принципиальные рекомендации:

• системы с программируемыми модулями имеют лучшую защиту от отказов по общей причине. Поэтому использование параметров моделей отказов по общей причине, полученных для технологических систем на основе обработки и интерпретации эксплуатационной статистики, является слишком консервативным и некорректным. Исходя из этого, в проведенном анализе использовались меньшие значения параметров моделей отказов по общей причине, чем при проведении ВАБ для Балаковской АЭС;

• при использовании традиционного параметрического подхода к учету отказов по общей причине значения параметров их моделей зависят от наличия и качества непрерывной диагностики состояния устройств системы и использования принципа разнообразия при разработке резервируемых элементов. В стандарте МЭК [7] в качестве такой параметрической модели рекомендуется применять модель бета-фактора. При использовании модели бета-фактора рассматривается отказ всей группы элементов по общей причине, независимо от количества элементов в группе.

В рассматриваемой системе ИВС/СППБ принцип разнообразия использован не был, что несколько ухудшает защищенность системы против как отказов по общей причине, так и ошибок программного обеспечения. В соответствии с рекомендациями стандарта МЭК [7] значение бета-фактора такой системы в двухканальном исполнении не может быть меньше, чем 0,01.

tural types of redundant elements. The availability of such factors of «generality» could lead to significant increase of the probability of the multiple failures.

Taking into account that the redundant elements of the ICS/SPPS system are located in one area (room of MCR, ECR or ICS), the important source of occurrence of the common cause failures could be connected with external influencing factors, such as moist-thermal and impact-vibration factors [6]. The equipment of the system is delivered in fire resistant and seismic stable implementation, and the air conditioning systems in MCR and ECR are operated permanently. Thus, it is assumed that the influence of the above-mentioned factors on the elements of the system will be minimum. But the practice shows that it is not possible to eliminate fully the common mode failures.

Usually in the reliability models only those common mode failures are taken into account, which occur simultaneously or in short periods of time, not exceeding by duration the specific time periods, determined by the reliability model (mean time of recovery for explicit failures and period of tests for hidden failures in the waiting mode). This is actual most of all for programmed instrumentation and control systems, for which the internal diagnostics of individual devices and cross check of redundant elements are envisaged with high degree of periodicity (i.e. practically continuously).

There are no domestic normative documents on practical accounting of common mode failures of the programmed systems. In IEC standard [7], which is today the only international normative document in this area, two principal recommendations are formulated:

• The systems with programmed modules have better protection from common mode failure. Thus the application of the parameters of models of common mode failures, received for technological systems on the basis of processing and interpretation of the operating statistics, is too conservative and incorrect. For this reason in the analysis fulfilled the less values of the parameters of models of common mode failures than during the conduction of PAS for Balakovo NPP, were used.

• During the application of traditional parametric approach to accounting the common mode failures the parameters values of their models depend on availability and quality of continuous diagnostics of state of the system devices and on use of the diversity principle at the development of the redundant elements. In IEC standard [7] it is recommended to use the model of beta – factor as a parametric model. At application of the beta-factor model the common mode failure of the whole group of elements is considered independently of amount of the elements in the group.

In the reviewed system ICS/SPPS the diversity principle was not used, this deteriorates to some extent the protection of system from

С другой стороны, большинство элементов анализируемой системы ИВС/СППБ является непрерывно контролируемыми с высокой степенью выявления отказов, что обычно составляет 99% от общего числа отказов по экспертным оценкам стандарта МЭК [7]. В соответствии с рекомендациями этого стандарта значение бета-фактора для элементов двухканальной системы с высокой эффективностью постоянного контроля, разработанной без применения принципа разнообразия, оценивается как:

$$\beta_t = 0,99\,\beta_d + 0,01\,\beta_u,$$

где β_t – суммарный бета-фактор;

β_d – бета-фактор 0,01 для обнаруживаемой части отказов;

β_u – бета-фактор 0,05 для необнаруживаемой части отказов.

При формировании групп элементов, подверженных отказам по общей причине, были приняты во внимание общность конструкции, общность расположения элементов и критерии отказа системы ИВС/СППБ. Учет последнего принципа привел к тому, что элементы одного типа образовали несколько групп, т.к. отказ только части однотипных элементов уже приводит к реализации вершинного события, т.е. к невыполнению системой заданных функций в соответствии со сформулированными критериями ее отказа. При этих граничных условиях формирование одной глобальной группы однотипных элементов, подверженных отказам по общей причине, привело бы к недооценке их вклада при использовании модели бета-фактора. Перечень групп элементов, подверженных отказам по общей причине и рассмотренных в модели, включает следующие элементы:

- жидкокристаллические мониторы;
- кабельная укладка и шлейфы блоков питания;
- внешние и внутренние блоки расширения;
- жесткие диски, устройства ввода, материнские платы, сетевые карты, процессоры, видеокарты рабочих станций и альфа-сервера;
- переключатели питания и сетевые переключатели;
- батареи и зарядные устройства;
- коммутаторы HP8000;
- диски массивов и стойки дисков альфа-сервера;
- RAID контроллер альфа-сервера.

Одним из основных вкладчиков в отказы по общей причине считаются ошибки программного обеспечения, которые не учитываются в рекомендованных стандартом МЭК [7] значениях параметров моделей отказов по общей причине. Поэтому такие ошибки рассмотрены отдельно.

6. АНАЛИЗ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Согласно требованиям ОПБ-88/97 [1] (пп. 4.4.4.5 и 4.4.5.9) проекты управляющих систем безопасности и нормальной эксплуатации должны содержать анализ надежности функциони-

both common mode failures and errors of the software. In accordance with the recommendations of IEC standard [7] the beta-factor value of this system in two-channel implementation could not be less than 0,01.

From the other side, the majority of the elements of the reviewed system ICS/SPPS are continuously monitored with high degree of revealing the failures, this is usually equal to 99 % of the total amount of the failures by expert evaluations of IEC standard [7]. In accordance with the recommendations of this standard the beta-factor value for the elements of two-channel system with high efficiency of permanent monitoring being designed without application of the diversity principle is estimated as:

$$\beta_t = 0,99\,\beta_d + 0,01\,\beta_u,$$

where β_t – total beta-factor;

β_d – beta-factor 0,01 for detected part of failures;

β_u – factor 0,05 for undetected part of failures.

During the generation of the groups of elements, subjected to common mode failures the generality of design, generality of location of the elements and criteria of failure of ICS/SPPS system have been taken into account. Accounting of the latter principle led to the following: the elements of one type formed several groups, as the failure of only a part of similar elements has lead already to realization of the top event, i.e. to non-fulfillment by the system of the specified functions in accordance with the formulated criteria of its failure. At these boundary conditions of generating one global group of similar elements subjected to common mode failures would lead to underestimation of their contribution during application of the beta-factor model. The list of groups of the elements, subjected to common mode failures and reviewed in the model includes the following elements:

- liquid crystal monitors;
- cable routes and trains of supply units;
- external and internal extension units;
- hard disks, input devices, mother boards, network cards, processors, video cards of workstations and alpha server;
- supply switches and mains switches;
- batteries and chargers;
- commutators HP8000;
- disks of massive and racks of alpha server disks;
- RAID controller of alpha server.

One of the main contributors into common mode failures are the errors of the software, which are not taken into account in of parameter values of models for common mode failures recommended by IEC standard [7]. For this reason such errors are reviewed separately.

6. ANALYSIS OF RELIABILITY OF THE SOFTWARE

According to the requirements of OPB-88/97 [1] (i.i. 4.4.4.5 and 4.4.5.9) the projects of control safety systems and normal opera-

рования программных средств. Аналогичные требования для аналитиков, проводящих анализ систем АЭС, важных для безопасности, содержатся в документах МАГАТЭ [9,10].

Общепризнанно, что нельзя гарантировать безошибочное функционирование программного обеспечения (ПО) даже при значительных затратах разработчиков на стадии разработки и тестирования программно-технических средств [8].

Показатели надежности программных средств характеризуют их способность выполнять заданные функции в соответствии со спецификациями в условиях естественных отклонений, возникающих в среде функционирования и вызванных различными дестабилизирующими факторами. К числу указанных факторов относятся, в частности, изменения условий работы технических средств, их отказы и сбои, изменения во входных данных, изменения в распределении ресурсов памяти.

Выявление потенциальных дефектов ПО ИВС/СППБ и минимизация их числа проводятся при отладке и внедрении системы. Следует, однако, отметить, что комбинаторный характер обработки и накопления информации и множество условных переходов создают большое количество путей выполнения программой той или иной команды. Этим объясняется невозможность выявить абсолютно все программные ошибки на этапах тестирования и опытной эксплуатации, хотя большинство ошибок тем не менее выявляются во время тестирования средств на полигоне и во время пуско-наладочных работ. Остаточное число ошибок ПО моделируется в модели надежности ИВС/СППБ.

При анализе надежности ПО ИВС/СППБ могут быть рассмотрены два вида отказов ПО: сбои и глобальные ошибки программирования, потенциально приводящие к невыполнению функций системы сразу во всех резервируемых модулях [4]. Следует отметить, что глобальные ошибки программирования характерны для систем управления, находящихся в режиме ожидания. Рассматриваемая система эксплуатируется в режиме «он-лайн», т.е. глобальные ошибки ПО, не выявляемые сразу и приводящие к невыполнению функции системы при реализации не предусмотренных при программировании конфигураций и граничных условий, являются крайне маловероятными. Поэтому проявление любых ошибок ПО будет иметь характер сбоев, проявляющихся в «зависании» системы и, следовательно, достаточно быстро выявляемых.

Сбои ПО вызываются невыявленными программными ошибками, которые главным образом влияют на организацию обмена данными. Как следствие наличия таких ошибок программа выдает неправильные результаты, несмотря на то что входные данные удовлетворяют спецификации требований, например, из-за проблем с динамическим распределением ресурсов. При этом, хотя коренная причина некоторых отказов ПО не устраняется и в точно такой же ситуации отказ должен повториться, точное повторение данных и, соответственно, связан-

tion systems shall include the analysis of reliability of the program means functioning. Similar requirements for analysts fulfilling the analysis of NPP systems important to safety are formulated in IAEA documents [9,10].

It is conventionally accepted that it is not possible to guarantee failure-free functioning of the software (SW) even at significant expenses of the developers at the stage of development and testing of program-technical means [8].

The reliability factors of program means characterize their capability to execute the specified functions in accordance with specifications in conditions of natural deviations, occurring in medium of functioning and caused by different destabilizing factors. In particular, the changes of operating conditions of technical means, their failures and faults, changes in the input data, changes in distribution of the memory resources are related to the specified factors.

The reveal of potential defects in SW of ICS/SPPS and minimization of their amount are fulfilled during debugging and implementation of the system. But it should be noted that combinatory character of information processing and accumulation and variety of conditional transitions create great amount of ways for executing one or another command nby the program. This is the reason of impossibility to reveal absolutely all program errors at stages of testing and pilot operation, but nevertheless, the majority of errors are detected during testing of program means at polygon and during start-up and adjustment operations. The residual number of SW errors is simulated in the reliability model of ICS/SPPS.

During the reliability analysis of the software of ПО ICS/SPPS two types of SW failures could be considered: faults and global errors of programming, potentially leading to non-fulfillment of functions of the system in all redundant modules at once [4]. It should be noted that global errors of programming are characteristic for control systems staying in waiting mode. The system reviewed is operated in «on-line» mode, i.e. global errors of the software, not revealed at once and leading to non-fulfillment of functions of the system during realization of configurations and boundary conditions not envisaged during programming, are extremely improbable. Thus exhibiting of any SW errors will be demonstrated as failures occurring in the form of «hanging up» of system and, consequently, will be revealed rather quickly.

The SW failures are caused by non-revealed program errors, which have influence mainly on organization of the data exchange. As the consequence of availability of such errors, the program delivers incorrect results despite the fact that the input data satisfies the specification of the requirements, for example, due to some problems with the dynamic distribution of resources. In this case though the root reason of some SW failures is not eliminated, and in exactly the same situation the failure should

ного с ним отказа маловероятно. Поэтому указанная ошибка программирования проявляется в виде перемежающихся отказов, т.е. сбоев, которые устраняются преимущественно автоматизированными методами (повторной инициализацией программы).

Так как резервируемые программные модули разработаны без использования принципа разнообразия и технические средства, на которых они установлены, являются идентичными, то предполагается, что отказ типа «зависания» будет возникать одновременно на обоих каналах системы, что является консервативным предположением. Время перезагрузки оценивается экспертной величиной 15 минут с учетом предшествующих ей административных процедур.

Для оценки показателей надежности ПО средств ИВС/СППБ был изучен опыт эксплуатации их аналогов и проведен сбор информации по фактам отказов программного обеспечения модулей на действующих блоках. По информации разработчика, за 25 лет эксплуатации на 7 энергоблоках АЭС, построенных по советским проектам, отказы ПО таких систем отсутствовали. Таким образом, интенсивность сбоев ПО системы, которая составляет 7,1E-6 1/ч, получена для нулевой статистики с использованием теоремы Байеса в предположении неинформативного априорного распределения.

7. ОЦЕНКА ВЕРОЯТНОСТИ ПОТЕРИ ВНЕШНЕГО ЭЛЕКТРОСНАБЖЕНИЯ СИСТЕМЫ

Система ИВС/СППБ подключена к сети бесперебойного электроснабжения. При перебоях электроснабжения питание системы обеспечивается от аккумуляторной батареи в режиме разряда. Во время обесточивания энергоблока аккумуляторная батарея остается единственным источником электроснабжения системы, которая может обеспечивать электроснабжение системы в течение одного часа. Кроме того, система оборудована собственными источниками бесперебойного питания, которые могут обеспечивать электроснабжение элементов системы еще в течение получаса после истощения аккумуляторной батареи энергоблока. Таким образом, полная потеря внешнего питания системы переменным током может произойти только при длительном обесточивании энергоблока (потере питания от внешних источников).

При анализе надежности ИВС/СППБ в условиях обесточивания, для которого возможно устранение первопричины исходного события, определена не только частота его возникновения, но и вероятность восстановления внешнего электроснабжения за 1–1,5 часа. Это позволило получить более реалистические значения вероятности отказа системы из-за этого исходного события.

Частота обесточивания энергоблока оценена по статистическим данным ВНИИАЭС, накопленным информационной системой по нарушениям в работе АЭС, где содержится информация о событиях на АЭС с ВВЭР-1000 России и

be repeated, the exact repetition of the data and, correspondingly, of the failures connected with it is improbable. Thus the specified error of programming is occurred in the form of alternated failures, i.e. faults, which are eliminated preferentially by automated methods (by repeated initialization of the program).

As the redundant program modules have been developed without application of the diversity principle, and the technical means, where they are installed, are identical, it is assumed that the failure of «hanging up» type will occur simultaneously at both channels of the system, this assumption is a conservative one. The time of reboot is estimated by experts as equal to 15 minutes with regard for previous administrative procedures.

For estimating the factors of the SW reliability of ICS/SPPS technical means the operating experience of their analogs has been studied, and the accumulation of information on events of failures of the software of the modules at the operating Units has been performed. According to the information of the developer during 25 years of operation at 7 power Units of NPPs, constructed by the Soviet projects, the failures of the software of these systems were absent. Thus, the intensity of SW failures of the system, which is equal to 7,1E-6 1/h, has been obtained for null statistics with the application of Bayes theorem in assumption of non-informative a priori distribution.

7. ESTIMATION OF PROBABILITY OF LOSS OF EXTERNAL ELECTRIC SUPPLY OF THE SYSTEM

The ICS/SPPS system is connected to the mains of uninterruptible electric supply. At interruptions of electric supply the system supply is provided from accumulator battery in discharge mode. During the power Unit de-energizing the accumulator battery is the only source of the electric supply of the system; the accumulator battery could provide the electric supply of the system during one hour. Besides, the system is equipped with intrinsic uninterruptible supply sources, which could provide the electric supply of elements of the system during half an hour after expiration of the accumulator battery of power Unit. Thus, full loss of external electric supply of the system with alternating current could occur only at durable de-energizing of power Unit (loss of electric supply from external supply sources).

During the analysis of the ICS/SPPS reliability in conditions of de-energizing, for which the elimination of the primary cause of initial event is possible, not only the rate of its occurrence has been determined but the probability of restoration of the external electric supply during 1–1,5 hours as well. This has permitted to receive more realistic values for probability of the system failure due to this initial event.

The rate of the power Unit de-energizing has been estimated on the basis of statistical

Украины, включая специфические данные с Балаковской АЭС. Оценка частоты обесточивания энергоблока выполнена с применением байесовской процедуры, используя опыт эксплуатации АЭС с ВВЭР-1000.

Для оценки вероятности восстановления электроснабжения при обесточивании энергоблока использована функция распределения времени восстановления питания от внешних источников для АЭС бывшего СССР, которая была определена на основании анализа всех отчетов о нарушениях в работе АЭС, занесенных в отечественную базу данных [11].

8. РЕЗУЛЬТАТЫ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ НАДЕЖНОСТИ ИВС/СППБ И ВЫВОДЫ

Дерево отказов системы ИВС/СППБ, разработанное в формате программы RiskSpectrum PSA Professional, было использовано для проведения количественной оценки надежности системы. Получено, что средняя оценка неготовности системы ИВС/СППБ составляет 1,79E-5. Практически полностью это значение определяется вкладом отказов по общей причине.

Анализ чувствительности показал, что основными вкладчиками в неготовность системы ИВС/СППБ являются следующие события:

- отказ по общей причине всех 4 мониторов рабочих станций на панелях расхолаживания РЩУ (вклад в общую оценку неготовности – 22,4%);
- отказ программного обеспечения системы ИВС/СППБ (вклад в общую оценку неготовности – 9,9%);
- обесточивание системы ИВС/СППБ продолжительностью более 1,5 часа (вклад в общую оценку неготовности – 4,4%).

Следует отметить, что неготовность системы оценена с использованием данных ее разработчика, основанных на гарантийном сроке элементов из-за отсутствия эксплуатационной информации и представляющихся чересчур консервативными. Поэтому эту оценку неготовности системы следует рассматривать как верхнюю.

ЛИТЕРАТУРА

1. Общие положения обеспечения безопасности атомных станций ОПБ-88/97. НП-001-97 (ПНАЭ Г-01-011-97), Госатомнадзор России, Москва, 1997.

2. Требования к управляющим системам, важным для безопасности атомных станций. НП-026-01. Госатомнадзор России, Москва, 2001.

3. **Швыряев Ю.В., Барсуков А.Ф., Деревянкин А.А., Морозов В.Б., Токмачев Г.В., Векслер Л.М.** Вероятностный анализ безопасности атомных станций. Методика выполнения. Ядерное общество СССР. Москва, 1992.

4. **Швыряев Ю.В., Морозов В.Б., Токмачев Г.В., Байкова Е.В.** Результаты откорректиро-

data of VNIIAES, accumulated by information system on disturbances in operation of NPPs where the information on events at NPPs with VVER-1000 of Russia and Ukraine, including specific data from Balakovo NPP, is contained. The estimation of the rate of power Unit de-energizing has been fulfilled with the application of Bayes procedure, using the operating experience of NPP with VVER-1000.

For estimating the probability of restoration of electric power supply at power Unit de-energizing the distribution function of restoring the supply from external sources for NPPs of the former USSR has been used; this function has been determined on the basis of analysis of all the reports on disturbances in NPPs operation introduced into domestic database [11].

8. RESULTS OF QUANTITATIVE ESTIMATION OF ICS/SPPS RELIABILITY AND CONCLUSIONS

The tree of failures of ICS/SPPS system, developed in format of program RiskSpectrum PSA Professional, has been used for fulfilling the quantitative estimation of the system reliability. It has been received that mean estimation of the unavailability of ICS/SPPS system is equal to 1,79E-5. This value is practically fully determined by the contribution of the common mode failures.

The analysis of the sensitivity has demonstrated that the following events are the main contributors into the unavailability of ICS/SPPS system:

- common mode failure of all 4 monitors of the workstations at the cooling panels in ECR (contribution to total estimation of the unavailability – 22,4%);
- failure of the software of ICS/SPPS system (contribution to total estimation of the unavailability – 9,9%);
- de-energizing of ICS/SPPS system with duration of more than 1,5 hours (contribution to total estimation of the unavailability – 4,4%).

It should be noted that the unavailability of the system is estimated with application of the data received from the developer, based on guarantee period of the elements due to absence of operational information and seems to be too conservative. Thus, this estimation of the unavailability of the system shall be reviewed as the top one.

REFERENCES

1. General statements of providing the safety of nuclear plants OPB-88/97. NP-001-97 (PNAE G-01-011-97), Gosatomnadzor of Russia, Moscow, 1997.

2. Requirements for control systems important to safety of nuclear plants. NP-026-01. Gosatomnadzor of Russia, Moscow, 2001.

3. **Yu.V.Shvyryaev, A.F. Barsukov, A.A. Derevyankin, V.B.Morozov, G.V.Tokmachev, L.M.Veksler.** Probabilistic safety analysis of nuclear plants. Procedure of fulfillment. USSR Nuclear Society. Moscow, 1992.

ванного ВАБ для АЭС повышенной безопасности с ВВЭР-1000. Седьмой международный форум по обмену информации «Анализ безопасности АЭС с реакторами типа ВВЭР и РБМК» (ФОРУМ-7), 28–30 октября 2003, Словакия.

5. Верификационный отчет программного средства RISK SPECTRUM PSA Professional версия 1.1. Атомэнергопроект. – Москва, 2001

6. **Черкасов Г.Н.** Надежность аппаратно-программных комплексов. Питер, Санкт-Петербург, 2005.

7. Международный стандарт 61508-6. «Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3». Международная электротехническая комиссия, Женева, Швейцария, 2000.

8. **Токмачев Г.В., Токмачев И.Г.** Надежность программного обеспечения систем безопасности АЭС. Атомная техника за рубежом. – Москва, 2004, № 12. – С. 3–14.

9. МАГАТЭ «Review of Probabilistic Safety Assessments in Regulatory Bodies». – Серия отчетов по безопасности. Отчет № 25, Вена, 2002.

10. МАГАТЭ «Software for Computer Based Systems Important to Safety of Nuclear Power Plants» – Серия стандартов МАГАТЭ по безопасности. Руководство по безопасности № NS-G-1.1, Вена, 2000.

11. **Морозов В.Б., Токмачев Г.В.** «Derivation of Frequency and Recovery Probabilities for Loss of Off-Site Power Accident». Труды Международной конференции по безопасности и надежности ESREL'97, 17–20 июня 1997 г., Лиссабон, Португалия, том 3. – С. 1889–1894, Elsevier Science, 1997.

4. **Yu.V.Shvyryaev, V.B.Morozov, G.V.Tokmachev, E.V.Baykova.** Results of corrected PSA for NPP of increased safety with VVER-1000. The seventh International Forum on Information Exchange. «Analysis of safety of NPP with reactors of VVER and RBMK types» (FORUM-7), October 28-30, 2003, Slovakia).

5. Verification report of program means RISK SPECTRUM PSA Professional version 1.1. Atomenergoproekt. Moscow, 2001.

6. **G.N. Cherkasov.** Reliability of hardware-software complexes. Peter, Saint-Petersburg, 2005.

7. International standard 61508-6. «Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3». International Electrotechnical Commission, Geneva, Switzerland, 2000.

8. **G.V. Tokmachev, I.G. Tokmachev.** Reliability of software of NPP safety systems. Atomic technique abroad, Moscow, 2004, No.12, p.p. 3-14.

9. IAEA «Review of Probabilistic Safety Assessments in Regulatory Bodies». – Series of safety Reports, Report No.25, Vienna, 2002.

10. IAEA «Software for Computer Based Systems Important to Safety of Nuclear Power Plants» - Safety Series of IAEA standards. Safety Guide No.NS-G-1.1, Vienna, 2000.

11. **V. Morozov, G.Tokmachev.** «Derivation of Frequency and Recovery Probabilities for Loss of Off-Site Power Accident». Proceedings of International Conference on Safety and Reliability ESREL'97, June 17-20, 1997, Lisbon, Portugal, volume 3, p.p.1889-1894, Elsevier Science, 1997.