

УДК 004.004.052.3

ОЦЕНКА НАДЁЖНОСТИ ИНФОРМАЦИОННО-ДИАГНОСТИЧЕСКОГО КОМПЬЮТЕРНОГО КОМПЛЕКСА

А.П. Галеев, А.А. Майоров, С.Г. Семенцов, В.Т. Семёнов

На примере промышленного варианта комплекса специального назначения ЭКСПРО, используемого для обработки и представления информации на объектах атомной энергетики, демонстрируется применение метода оценки надёжности информационно-диагностических компьютерных комплексов. Метод включает оценку надёжности аппаратуры, тестирование и оценку безотказного функционирования программного обеспечения. Предложена методика тестирования аппаратного обеспечения комплекса. Предложена структурная схема для расчёта надёжности комплекса. Проведён расчёт надёжности комплекса, включающий в себя как надёжность системного программного обеспечения, так и аппаратного обеспечения. Разработана статистическая модель функции надёжности комплекса от времени эксплуатации. Показано, что расчётная надёжность удовлетворяет заданным требованиям в течение всего периода эксплуатации комплекса.

Ключевые слова: надёжность программного обеспечения, аппаратно-программный комплекс, резервирование, системное программное обеспечение, расчёт надёжности.

В современном мире информационно-технические комплексы (ИТК) на основе компьютеров широко применяются для управления и диагностики функционирования различных объектов. Показатели надёжности входят в число обязательных требований при разработке радиоэлектронных систем (РЭС), в том числе и ИТК с применением компьютеров.

Особенностью ИТК является наличие в них в совокупности с аппаратными средствами программного обеспечения (ПО), которое функционирует с помощью компьютера. Опыт создания сложных информационных систем в последние десятилетия выявил множество ситуаций, при которых сбои и отказы их функционирования были обусловлены не только дефектами аппаратуры, но и недостатками комплексов компьютерных программ. Соответственно, надёжность работы информационно-технического комплекса определяется как надёжностью технических средств – аппаратуры, так и надёжностью ПО.

Вторая составляющая общей надёжности ИТК – надёжность ПО – является не менее важной, чем надёжность аппаратных средств. В настоящее время уже накоплен значительный опыт определения надёжности программных средств, применяемых в авиационной, космической, атомной и других областях современной высокоинтеллектуальной техники. В этих областях недопустимо для тестирования и определения надёжности ПО использовать функционирование реальных объектов. В связи с этим при испытаниях на надёжность создаются моделирующие испытательные стенды на базе программных модулей и компонентов реальных объектов. Стенды позволяют определить надёжность функционирования конкретного ПО в условиях штатных и критических внешних воздей-

ствий, соответствующих реальным характеристикам внешней среды.

В данной работе показано применение метода оценки надёжности ИТК, включающего оценку надёжности аппаратуры и ПО, для случая с требованиями обеспечения чрезвычайно высокого уровня надёжности, безотказности и безопасности объекта, а именно для комплекса системы управления защитой атомных электростанций.

Объект исследования

Объект исследования с целью оценки надёжности – информационно-диагностическая система, являющаяся совокупностью системного ПО и аппаратных средств.

Использовался информационно-диагностический компьютерный комплекс специального назначения ЭКСПРО (ИДККСН ЭКСПРО), применяемый на объектах атомной энергетики. Создан ВНИИЭМ на основе компьютера с архитектурой PC AT (Personal Computer Advanced Technology – персональный компьютер класса AT). Изготавливается в усиленном промышленном исполнении и предназначен для обработки и представления информации по задаваемым алгоритмам в тяжёлых условиях эксплуатации автономно или в составе измерительных, вычислительных, информационных, управляющих и иных автоматических и автоматизированных систем, в том числе на объектах атомной энергетики (ККСН ЭКСПРО соответствует требованиям класса ЗН по ПНАЭГ-1-011-89/97) [1, 2].

Конструкция комплекса. В конструкцию комплекса входят (рис. 1):

– основная рабочая станция PC 1 TW, предназначенная для тестирования и контроля аппаратно-

го и программного обеспечения, для отработки техник резервирования, обеспечения живучести, восстановления после сбоя;

– резервная рабочая станция PC 2 PW – для осуществления горячего резервирования (информационный поток, поступающий на рабочую станцию PC 1 TW, копируется на резервную PC 2 PW);

– сервер диагностической информации PC/104 – РСМ-3341 (ЭВМ стандарта PC 104), формирует информационный поток от органов регулирования в виде IPX-пакетов и имитирует сигналы, поступающие с датчиков атомной электростанции;

– сетевой коммутатор 3 COM SuperStack 3 Switch 3870 (устройство, объединяющее компьютеры в сеть и позволяющее направить поступивший в них сигнал только на тот порт, к которому подключён данный компьютер) – для обмена информацией между серверами и аппаратно-программными имитаторами;

– источник бесперебойного питания Powerware 3.

Программное обеспечение. ИДККСН ЭКСПРО функционирует на базе операционной системы (ОС) LiNem.

LiNem – специализированная операционная система для систем управления и защиты АЭС [3 – 5]. Это – специализированный дистрибутив (т. е.

форма распространения системного ПО (СПО), предназначенный для работы в составе программно-технического комплекса информационно-диагностической сети системы управления защитой атомных реакторов. Создан на основе операционной системы Linux. В связи с большим количеством разнообразного коммуникационного оборудования и сложной структурой интерфейсов в составе ИДККСН ЭКСПРО поддержание работы сети невозможно без системы диагностики и управления, которая в автоматическом режиме собирает информацию о состоянии оборудования и ПО, входящего в сеть, создаёт архив, предоставляет эту информацию оператору сети и на основе этой информации осуществляет управление.

Для решения этой задачи в составе дистрибутива LiNem разработана специализированная подсистема контроля и диагностики – программа обеспечения живучести (ПОЖ). Система управления работает в автоматизированном режиме, выполняя большую часть действий по управлению оборудованием и программным обеспечением сети автоматически, а такие действия, как переустановка ПО, замена оборудования выполняются человеком-оператором на основе подготовленной системы информации. Программы, входящие в ПОЖ, выполняют:



Рис. 1. Структурная схема ИДККСН ЭКСПРО

- включение ИДККСН ЭКСПРО в работу;
- диагностику программных и аппаратных средств комплекса;
- обеспечение работы комплекса в режиме горячего резервирования;
- ведение архива состояния комплекса;
- оперативную переустановку ПО в случае отказов и сбоев программных и аппаратных средств.

Схема информационного обмена ИДККСН ЭКСПРО представлена на рис. 2.

Информационный поток (диагностическая информация) от органов регулирования в виде IPX-пакетов формируется с помощью сервера PC 104 и поступает на коммутатор. Сервер также имитирует сигналы с датчиков АЭС, которые заводятся через плату цифрового ввода на основную рабочую станцию (интерфейс «токовая петля»). Обработанные на рабочей станции данные копируются на резервную станцию с помощью программы зеркалирования. Обмен между рабочей и резервной станциями по протоколу TCP/IP необходим для контроля функционирования СПО на аппаратном уровне. Сетевой протокол IPX управляет адресацией и направлением пакетов между локальными сетями и в их пределах. Набор сетевых протоколов TCP/IP поддерживает связь между объединёнными сетями из

компьютеров различной архитектуры и с разными операционными системами, включает в себя стандарты для связи между компьютерами и соглашения о соединении сетей и правилах маршрутизации сообщений.

Методика оценки надёжности ИДККСН ЭКСПРО

Надёжность ИДККСН ЭКСПРО оценивалась по основному показателю безотказности – вероятности безотказной работы комплекса [6, 7]. Определялись:

- вероятность безотказной работы аппаратуры комплекса, P_4 по исходным данным от производителей аппаратуры и комплектующих изделий ИДККСН ЭКСПРО – по значениям средней наработки на отказ;
- вероятность безотказного функционирования системного программного обеспечения (СПО) LiNem, $P_{СПО}(t)$, – по результатам квалификационных испытаний комплекса;
- вероятность безотказной работы всей информационной системы ИДККСН ЭКСПРО, определяемой вероятностью совместных событий – безотказной работой аппаратуры и безотказным функционированием СПО LiNem:

$$P_{ис}(t) = P_4(t)P_{СПО}(t).$$

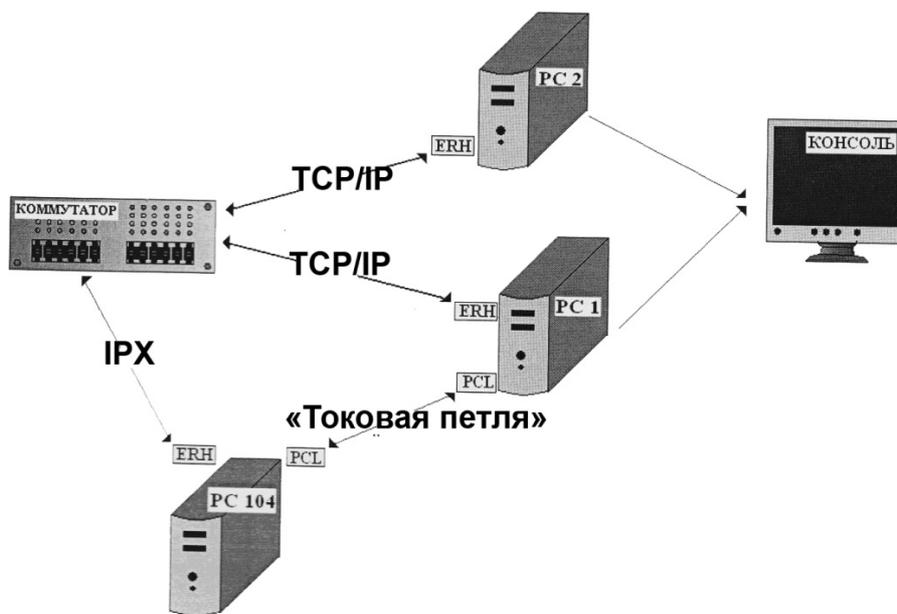


Рис. 2. Схема информационного обмена ИДККСН ЭКСПРО: ERH – сетевой интерфейс; PCL – плата ввода-вывода

Методика проведения квалификационных испытаний

Цель испытаний – проверка работоспособности и устойчивости функционирования информационно-диагностической системы, являющейся совокупностью системного программного обеспечения LiNem и аппаратных средств этого комплекса, при типовом режиме работы комплекса и в режиме тестовых нагрузок. Проверяется функционирование СПО LiNem и совместимость аппаратуры и СПО LiNem.

Испытания можно условно разделить на два этапа. Первый этап – тестирование СПО LiNem. Испытания проводились под искусственно созданной нагрузкой, изменяемой случайным образом, с помощью экспериментального тестового набора CTCS (Cerberus Test Control System). Тестовый набор разработан на основе анализа статистики наиболее часто встречающихся ошибок в драйверах устройств, системном ПО и аппаратном обеспечении. Тесты провоцируют возникновение ошибок при нагрузке на процессор, память, дисковую подсистему и системные шины.

Второй этап – проверка совместимости СПО LiNem и оборудования ИДККСН ЭКСПРО. Испытания проводились с помощью тестов ОНСР (Open Hardware Certification Program), LTP (Linux Testing Project) и linem-tests, непосредственно тестирующего оборудование: память, центральный процессор, материнскую плату; дисковую подсистему; видеоподсистему; сетевую подсистему.

Тесты LTP и ОНСР широко используются для проверки операционных систем на основе ОС Linux на соответствие действующим стандартам. Они применяются разработчиками программного обеспечения для проверки корректности функционирования ОС на различных аппаратных средствах. Представляют собой набор специально разработанных программ для тестирования «живучести» программно-аппаратных комплексов в штат-

ном режиме и в состоянии искусственно создаваемых нагрузок.

Тестирование работы с окнами и режимами работы видеокарт проводилось с помощью теста VSW5 вместе с тестом CTCS.

Тест linem-tests специально разработан НПП ВНИИЭМ для испытаний СПО LiNem. Испытания ИДККСН ЭКСПРО проводились в течение 100 ч.

Оценка надёжности аппаратуры ИДККСН ЭКСПРО

Оценка надёжных характеристик аппаратного обеспечения проводилась по методике расчёта надёжности сложных систем.

Структурная схема для расчёта надёжности ИДККСН ЭКСПРО представлена на рис. 3, она состоит из четырёх основных блоков: сервера PC/104; коммутатора; основной рабочей станции PC 1 TW; резервной рабочей станции PC 2 HW.

В работе комплекса используется горячее резервирование, когда основная и резервная рабочие станции работают в одинаковых режимах.

Расчёт проводится с использованием экспоненциальной модели надёжности. Надёжность аппаратуры ИДККСН ЭКСПРО оценивается по показателю – вероятность безотказной работы – в соответствии с представленной структурной схемой надёжности, т. е. рассчитывается вероятность безотказной работы системы при последовательном соединении блоков: коммутатор – линия связи с сервером – сервер PC/104 – параллельно соединённые рабочие станции с последовательными линиями связи.

В табл. 1 представлены исходные данные от производителей аппаратуры и комплектующих изделий ИДККСН ЭКСПРО для расчёта надёжности блоков структурной схемы – средние наработки на отказ отдельных блоков аппаратуры и комплектующих элементов, а также значения интенсивности

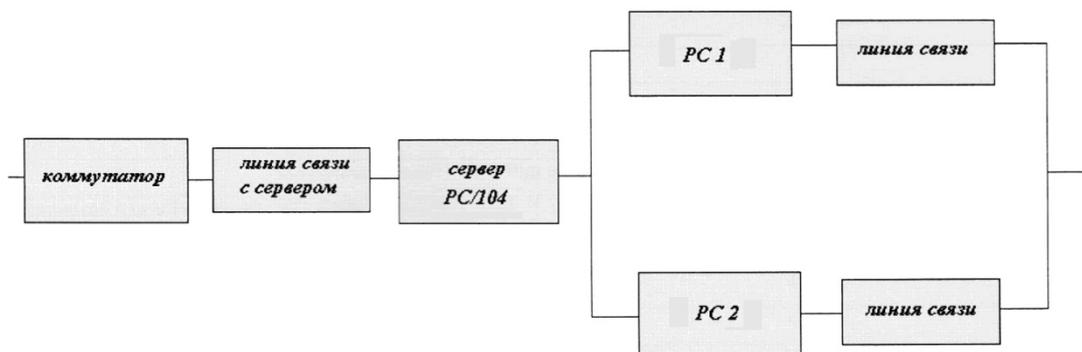


Рис. 3. Структурная схема для расчёта надёжности ИДККСН ЭКСПРО

Таблица 1

Средняя наработка на отказ и интенсивность отказов блоков и элементов ИДККСП ЭКСПРО

Элемент, блок	Средняя наработка на отказ, \bar{t}_i , (данные от производителей аппаратуры и элементов)	Интенсивность отказов, λ_i , 1/ч ($\lambda_i = 1/\bar{t}_i$)
Сервер PC/104 – РСМ-3341	198 000	$\lambda_{PC104} = 5,05 \cdot 10^{-6}$
Сетевой коммутатор 3 COM SuperStack 3 Switch 3870	268 000	$\lambda_{КОМ} = 3,73 \cdot 10^{-6}$
Источник бесперебойного питания Powerware 3	60 000	$1,7 \cdot 10^{-5}$
Сетевой кабель 100Base-TX	131 400	$\lambda_{ЛС} = 7,61 \cdot 10^{-6}$
Комплекующие основной рабочей станции РС 1		
Материнская плата Portwell ROBO-8710VLA-01 (чипсет Intel 845)	109 211	$9,16 \cdot 10^{-6}$
Центральный процессор Celeron 1700	43 800	$2,28 \cdot 10^{-5}$
Оперативная память Kingston DIMM 512 Мб	50 000	$2,0 \cdot 10^{-5}$
Носитель на жёстких магнитных дисках Seagate Barracuda ST 3160023A ёмкостью 160 Гб	183 000	$5,46 \cdot 10^{-6}$
Носитель на гибких магнитных дисках Mitsumi D359 M3D ёмкостью 1,44 Мб	100 000	10^{-5}
Сетевой адаптер 3COM 3C905-TX-M	226 000	$4,42 \cdot 10^{-6}$
Сетевой контроллер Allied Telesyn AT-2746FX/ST	46 000	$2,17 \cdot 10^{-5}$
Контроллер ввода Advantech PCL-733	30 000	$3,33 \cdot 10^{-5}$
Контроллер вывода Advantech PCL-741	30 000	$3,33 \cdot 10^{-5}$
Комплекующие резервной рабочей станции РС 2		
Материнская плата Portwell ROBO-679K-10 (чипсет Intel 810e)	95 000	$1,05 \cdot 10^{-5}$
Центральный процессор Celeron 667	42 000	$2,38 \cdot 10^{-5}$
Оперативная память Kingston DIMM 256 Мб	48 000	$2,08 \cdot 10^{-5}$
Носитель на жёстких магнитных дисках Seagate U Series5 ST 340823A ёмкостью 60 Гб	180 000	$5,56 \cdot 10^{-6}$
Носитель на гибких магнитных дисках Mitsumi D359 M3 ёмкостью 1,44 Мб	100 000	10^{-5}
Сетевой адаптер 3COM 3C980C-TX-M	230 000	$4,35 \cdot 10^{-6}$
Сетевой контроллер Portwell Robo-U160H	52 000	$1,92 \cdot 10^{-5}$
Контроллер ввода Advantech PCL-733	30 000	$3,33 \cdot 10^{-5}$
Контроллер вывода Advantech PCL-735	30 000	$3,33 \cdot 10^{-5}$

отказов, рассчитанные по значениям средней наработки на отказ. Результаты расчёта интенсивности отказов и вероятности безотказной работы блоков структурной схемы и всего комплекса сведены в табл. 2. Вероятность безотказной работы системы при последовательном соединении элементов (блоков) оценивается по формуле:

$$P_n(t) = \prod_{i=1}^n P_i(t) = e^{-\lambda_n t}, \quad (1)$$

где n – количество элементов; $P_i(t)$ – вероятность безотказной работы i -го элемента; $\lambda_n = \sum_{i=1}^n \lambda_i$ – интенсивность отказов системы, 1/ч; t – временной интервал, на котором рассчитывается надёжность, ч; $\lambda_i = 1/\bar{t}_i$ – интенсивность отказов i -го элемента, которая рассчитывается по величине средней наработки на отказ i -го элемента, \bar{t}_i .

Таблица 2

Интенсивность отказов и вероятность безотказной работы блоков структурной схемы и всего комплекса ИДККСН ЭКСПРО

Блоки	Интенсивность отказов, 1/ч	Вероятность безотказной работы
Станция РС 1: последовательно соединённые элементы станции	$\lambda_{PC1TW} = \sum_{i=1}^n \lambda_i = 1,6 \cdot 10^{-4}$ λ_i – интенсивность отказов i -го элемента (из табл. 1)	
РС 1 + линия связи (сетевой кабель 100Base-TX), последовательно соединённые	$\lambda_{ЛС} = 7,61 \cdot 10^{-6}$ (из табл. 1) $\lambda_{C1} = \sum_{i=1}^n \lambda_i = \lambda_{PC1TW} + \lambda_{ЛС} = 1,68 \cdot 10^{-4}$	$P_1(t) = P_{PC1TW}(t) \cdot P_{ЛС}(t) = e^{-\lambda_{C1} \cdot t}$ $P_1(t) = 0,9833$
Станция РС 2: последовательно соединённые элементы станции	$\lambda_{PC2PW} = \sum_{i=1}^n \lambda_i = 1,61 \cdot 10^{-4}$	
РС 2 + линия связи (сетевой кабель 100Base-TX), последовательно соединённые	$\lambda_{C2} = \sum_{i=1}^n \lambda_i = \lambda_{PC2PW} + \lambda_{ЛС} = 1,69 \cdot 10^{-4}$	$P_2(t) = P_{PC2PW}(t) \cdot P_{ЛС}(t) = e^{-\lambda_{C2} \cdot t}$ $P_2(t) = 0,9832$
Параллельно соединённые станции РС 1 и РС 2 со своими линиями связи (2 и 4)		$P_3(t) = 1 - [1 - P_1(t)] \cdot [1 - P_2(t)]$ $P_3(t) = 0,9997$
Комплекс ЭКСПРО (последовательно соединённые блоки комплекса ЭКСПРО: коммутатор – линия связи – сервер РС/104 – параллельно соединённые станции РС 1 и РС 2 с их линиями связи)	$\lambda_{КОМ} = 3,73 \cdot 10^{-6}$ $\lambda_{PC104} = 5,05 \cdot 10^{-6}$ $\lambda_{ЛС} = 7,61 \cdot 10^{-6}$ (из табл. 1)	$P_4(t) = P_{КОМ}(t) \cdot P_{PC104}(t) \cdot P_{ЛС}(t) \cdot P_3(t)$ $P_{КОМ}(t) = e^{-\lambda_{КОМ} \cdot t} = 0,9996$ $P_{PC104}(t) = 0,9995$ $P_{ЛС}(t) = 0,9992$ $P_3(t) = 0,9997$ $P_4(t) = 0,998$

Вероятность безотказной работы системы при параллельном соединении элементов оценивается по формуле:

$$P_m(t) = 1 - \prod_{i=1}^m [1 - P_i(t)], \quad (2)$$

где m – количество элементов.

Вероятность безотказной работы комплекса рассчитывается в соответствии с представленной структурной схемой в последовательности:

– последовательно соединённых РС 1 TW и её линии связи по (1);

– последовательно соединённых РС 2 TW и её линии связи по (1);

– параллельно соединённых РС 1 TW и РС 2 PW с их линиями связи по (2);

– последовательно соединённых блоков комплекса ЭКСПРО: коммутатора – линии связи – сервера РС/104 – параллельно соединённых станций РС 1 и РС 2 с их линиями связи по (1).

Расчёт показал высокий уровень надёжности аппаратуры ИДККСН ЭКСПРО с вероятностью безотказной работы 0,998 за период проведения тестирования 100 ч.

Оценка надёжности функционирования СПО LiNem

В табл. 3 приведены содержание и результаты тестирования СПО LiNem по перечисленным выше тестам, а в табл. 4 – распределение ошибок в процессе тестирования в течение 100 ч и расчётные показатели надёжности.

Оценивалась вероятность безотказного функционирования программного обеспечения – в соответствии с международным стандартом ГОСТ 28195-89 «Оценка качества программных средств. Общие положения», дата введения 01.07.90 [6]. Надёжность как показатель качества программных средств оце-

нивается вероятностью безотказного функционирования как основной характеристики устойчивости функционирования программных средств (способности обеспечивать продолжение работы программы после возникновения отклонений, вызванных сбоями технических средств, ошибками во входных данных и ошибками обслуживания).

Кроме вероятности безотказного функционирования программного обеспечения в табл. 4 приведены расчётные значения дифференциальных характеристик безотказности ПО: статистической интенсивности отказов и статистической плотности распределения наработки на отказ.

Таблица 3

Содержание и результаты тестирования СПО LiNem

Наименование проверок и испытаний. Критерий положительного результата	Тест	Результат испытания
<i>Проверка запуска и диспетчеризации не менее 20 задач.</i> Каждый из тестов должен закончиться успешно. Журнальный файл не должен содержать сообщений об ошибках	LTP, CTCS	Результат испытаний положительный. С ошибками закончились 3 теста из 45
<i>Поддержка разделяемой памяти.</i> Каждый из тестов должен закончиться успешно. Журнальный файл не должен содержать сообщений об ошибках	LTP, CTCS	Результат положительный
<i>Системный таймер:</i> задание временных задержек при выполнении программ. Требование ТЗ: точность таймера – не более 100 мс	LTP, CTCS	Результат положительный. Точность системного таймера платформы – 18 мс
<i>Обслуживание применяемых технических средств</i> (привода жёсткого диска, дисковод гибких дисков, видео- и сетевых адаптеров, монитора, клавиатуры, привода CD-ROM, ИБП)	ОНСР (для жёсткого диска, привода CD-ROM), CTCS	Результат положительный. Выводы тестов за фиксированный промежуток времени не содержат записей об ошибках
<i>Представление информации на мониторе ИДККСП ЭКСПРО или на подключённом принтере.</i> По окончании работы журнальный файл не должен содержать более 2% неуспешно завершившихся файлов	VSW5 для тестирования работы с окнами и режимами работы видеокарт, выполняемый вместе с тестом CTCS	Результат положительный
<i>Зеркалирование рабочих станций.</i> Файлы, передаваемые от основной рабочей станции на резервную. Проверка проводится путём сравнения тестовых данных, подлежащих зеркалированию, и их копий. Для каждого из 50 файлов размером 16 Кб в блоке находится контрольная сумма и после копирования сравнивается с контрольной суммой оригинала	Тест linem-test CTCS	Результат положительный. Вывод теста не содержит сообщений о несовпадении контрольной суммы файлов
<i>Поддержка протокола IPX.</i> Входная информация – IPX-пакеты, выходная информация – IPX-пакеты. Определяется стабильность передачи сигналов по протоколу IPX. Периодичность посылки тестовых IPX-пакетов – 1 с. Контролируется отсутствие случаев приёма файлов, содержащих случайную информацию, а также минимальное время прохождения пакетов данных	Тест linem-tests LTP, CTCS	Результат положительный. Количество несовпавших контрольных сумм не превышает 0,01% при частоте следования пакетов данных 1с (фактически неудачно завершено 0,007%)

Наименование проверок и испытаний. Критерий положительного результата	Тест	Результат испытания
<i>Поддержка протокола TCP/IP.</i> Проверка сетевых функций ПО проводится в режиме передачи/приёма потока данных с одновременным учётом параметров качества (точности приёма пакета, содержащего тестовую информацию и отсутствие приёма пакета со случайной информацией). Контролируется время обмена пакетами TCP/IP между основной и резервной станциями и коммутатором, число потерянных пакетов из 1000 (не должно быть потеряно более 0,01 % пакетов). Среднее время прохождения пакетов не должно превышать 12 мс	Тест linem-tests ОНСР, СТС	Результат положительный. Максимально допустимое время прохождения пакета данных было превышено для 2двух пакетов. Среднее время прохождения пакетов не превышало 12 мс
<i>Приём-передача информации через контроллеры ввода-вывода дискретных сигналов.</i> Процесс тестирования заключается в установке выходов платы PCL-735 в случайное состояние и считывании состояния входов платы PCL-733. Сравнивается состояние выходов платы PCL-735 и входов платы PCL-733. При идентичности показаний для всех диапазонов времени переключения результат положительный. Критерий – в журнальном файле должно быть не более 0,01% сбоев при передаче цифровых данных	Тест linem-tests (драйвера плат фирмы Advantech PCL-735 и PCL-735, выполняемый в течение фиксированного времени), СТС	Результат положительный. Цикл записи/чтения по 12 каналам не превышает 10 мс
<i>Защита от несанкционированного доступа</i> – обеспечение безопасности сети: пароли операторов, право доступа к системе. Вывод теста не должен содержать ни одного подобранного пароля по прошествии 10 ч	Тест linem-tests	Результат положительный. Вывод теста не содержит ни одного подобранного пароля по прошествии 10 ч

Значения статистической интенсивности отказов

$$\lambda_i = \frac{n_i}{(N - n_{i-1})t_i}, \quad (3)$$

где λ_i – статистическая интенсивность отказов, 1/ч; n_i – количество ошибок СПО в каждый i -й интервал времени тестирования; n_{i-1} – количество ошибок СПО в каждый $(i-1)$ -й интервал времени тестирования; t_i – длительность i -го интервала.

Статистическая плотность распределения наработки на отказ СПО

$$f(t) = \frac{n_i}{Nt_i}, \quad (4)$$

где N – общее число испытаний (тестов), $N = 128$.

Вероятность безотказного функционирования СПО оценивалась по формуле:

$$P_{\text{СПО}}(t) = 1 - \frac{n}{N}, \quad (5)$$

где n – число ошибок, зафиксированных при испытаниях.

Таким образом, вероятность безотказного функционирования СПО LiNem в течение времени тестирования, равного 100 ч, $P_{\text{СПО}}(100)$, составляет 0,93.

На основании проведённых испытаний и расчётов можно констатировать, что СПО LiNem соответствует требованиям по надёжности и безопасности.

Оценка надёжности ИДККСП ЭКСПРО

Теперь, зная вероятность безотказной работы аппаратуры ИДККСП ЭКСПРО $P_4(t) = 0,9982$ (см. табл. 2) и вероятность безотказного функционирования СПО LiNem $P_{\text{СПО}}(t) = 0,93$, определяем вероятность безотказной работы информационной системы ИДККСП ЭКСПРО в целом:

$$P_{\text{ИС}}(t) = P_4(t)P_{\text{СПО}}(t). \quad (6)$$

Вероятность безотказной работы информационной системы ИДККСП ЭКСПРО в целом в течение времени $t = 100$ ч

$$P_{\text{ИС}}(t) = 0,998 \cdot 0,93 = 0,928.$$

Таблица 4

Распределение ошибок в процессе тестирования СПО LiNem в течение 100 ч и расчётные показатели надёжности

Количество и наименование сбоев	Интервал времени i , ч			
	0 – 25	25 – 50	50 – 75	75 – 100
1 тест диспетчеризации 20 задач закончился с ошибкой; 1 несовпавшая контрольная сумма при передаче IPX пакета	1 пакет данных потерян; 2 несовпавшие контрольные суммы при передаче IPX пакета	2 теста диспетчеризации 20 задач закончились с ошибками	1 пакет данных потерян; 1 тест диспетчеризации 20 задач закончился с ошибкой	
Количество ошибок в каждый i -интервал времени тестирования, n_i	2	3	2	2
Статистическая интенсивность отказов λ_i , 1/ч (рис. 4)	$\lambda(0-25) = 0,000625$	$\lambda(25-50) = 0,000952$	$\lambda(50-75) = 0,00065$	$\lambda(75-100) = 0,00066$
Статистическая плотность распределения наработки на отказ, $f(t)$ (рис. 5)	$f(0-25) = 0,000625$	$f(25-50) = 0,000937$	$f(50-75) = 0,000625$	$f(75-100) = 0,000625$
Вероятность безотказного функционирования программного обеспечения, $P_{СПО}(t) = 1 - n / N, N = 128, n$ – число ошибок при испытаниях (рис. 6)	$P_{СПО}(25) = 0,984$ $n = 2$	$P_{СПО}(50) = 0,961$ $n = 5$	$P_{СПО}(75) = 0,945$ $n = 7$	$P_{СПО}(100) = 0,93$ $n = 9$

Зависимость статистической интенсивности отказов СПО от времени тестирования:

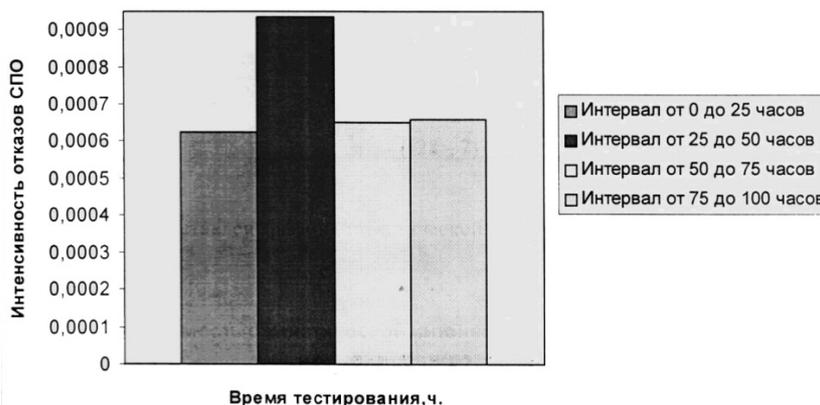


Рис. 4. Статистическая интенсивность отказов СПО LiNem

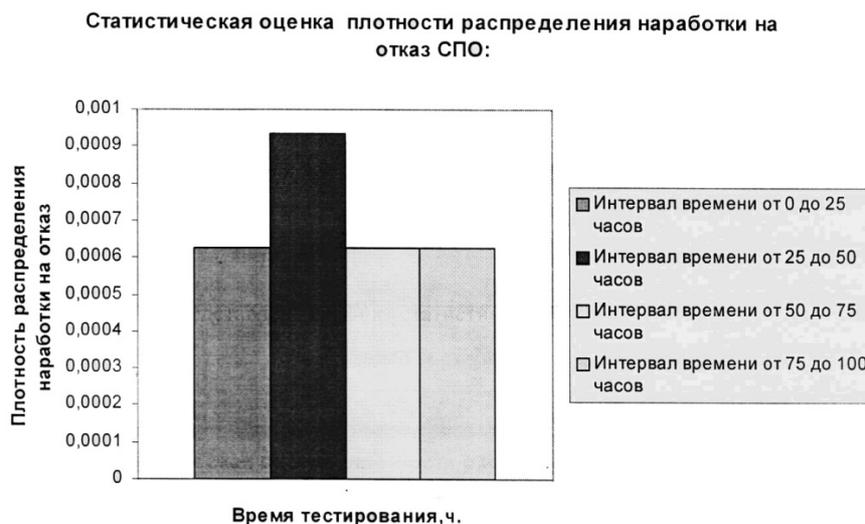


Рис. 5. Статистическая плотность распределения наработки на отказ СПО LiNem

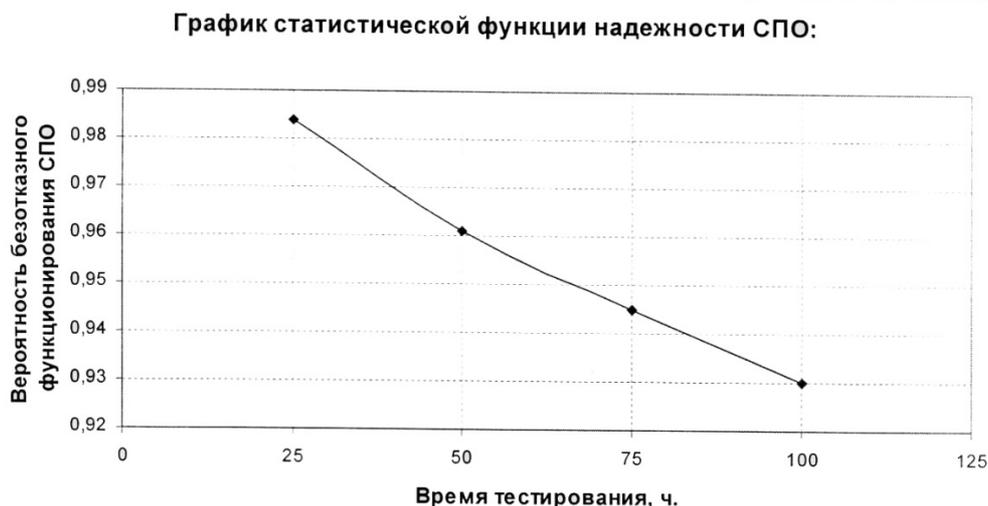


Рис. 6. Вероятность безотказного функционирования СПО LiNem

Заключение

Проведено тестирование и оценка надёжности промышленного варианта информационно-диагностического компьютерного комплекса, совмещающего в себе радиоэлектронное оборудование (аппаратуру) и компьютерные программы (программное обеспечение). Тестирование показало возможность появления ошибок и сбоев в работе программ, распределённых во времени случайным образом.

Вероятность безотказной работы информационной системы ИДККСП ЭКСПРО равна 0,928 (в течение времени тестирования 100 ч). Информационно-диагностический комплекс ЭКСПРО соответствует требованиям по надёжности и безопасности.

Обязательным условием обеспечения надёжности информационно-диагностических компьютерных комплексов должна быть оценка надёжности как аппаратуры, так и ПО. Требуется разработка стандартизированных методов и критериев оценки надёжности ПО таких систем. Предварительно необходимо исследование статистики отказов и сбоев различных ПО в течение длительного времени, установление законов распределения отказов и сбоев во времени и уточнение математических моделей оценки надёжности.

Международные стандарты в области качества продукции включают и вопросы стандартизации в области качества информационной продукции. В связи со стремительным развитием новых ин-

формационных технологий стандартизацией в этой области занимаются многие международные организации. Это, например, объединённый технический комитет стандартизации JTC 1, в котором 26 стран участвуют непосредственно и 33 страны присутствуют в качестве наблюдателей. Комитет создан в 1987 г. как результат совместных действий ISO и IEC (International Electrotechnical Commission). ISO – International Standards Organization – ведущая международная организация по стандартизации, включает 214 Технических комитетов [8].

Другие организации: Международный союз электросвязи ITU (International Telecommunications Union); Европейский институт телекоммуникационных стандартов ETSI (European Telecommunications Standards Institute); Европейский комитет по стандартизации CEN (Comité Européen de Normalisation); Европейский комитет электротехнической стандартизации CENELEC (Comité Européen de Normalisation Électrotechnique); Европейский институт по стандартизации в области телекоммуникаций ETSI (European Telecommunications Standards Institute) и др. [8].

Одним из основных назначений стандартизации является обеспечение и повышение качества продукции. Обеспечение качества информационной продукции включает обеспечение её надёжности. Для этого необходимо знать и использовать разнообразные методы оценки надёжности программной продукции. Это свидетельствует о значимости решения проблемы обеспечения надёжности программных средств и в первую очередь вопросов разработки методов оценки надёжности и стандартизации этих методов.

На примере промышленного варианта комплекса специального назначения ЭКСПРО, используемого для обработки и представления информации на объектах атомной энергетики, продемонстрировано применение метода оценки надёжности информационно-диагностических компьютерных комплексов. Метод включает оценку надёжности аппаратуры, тестирование и оценку безотказного функционирования ПО. Приняты некоторые упрощения, в частности не показано, как осуществляется аппаратный контроль работоспособности рабочих станций, переключение на резервный канал и автоматическое восстановление системы; не учитывались отказы блоков питания. Механизмы отслеживания работоспособности рабочих станций и переключения на резервный канал, работоспособность блоков питания тоже должны учитываться в структурной схеме надёжности.

За счёт процедуры автоматического восстановления системы после каждого сбоя программная составляющая устанавливается «с чистого листа», поэтому её влияние на суммарную надёжность комплекса будет меньше.

В методике расчёта отдельно считается надёжность аппаратных и программных средств. Но при возникновении сбоев и отказов не всегда удаётся выделить аппаратную и программную составляющие. Поэтому представляется логичнее считать общую надёжность аппаратно-программного комплекса.

В случае аппаратно-программных комплексов, предназначенных для обслуживания объектов ядерной энергетики, необходимо учитывать требования действующих нормативных документов (МЭК), предъявляемые к этим комплексам.

В каждом конкретном применении таких комплексов в методиках оценки надёжности необходимо отражать особенности аппаратного и программного обеспечения с использованием накопленного опыта исследований в области информационных технологий, в частности изложенного в работах [9 – 18].

Литература

1. Компьютерный комплекс специального назначения ЭКСПРО: [Электронный ресурс]: НПП ВНИИЭМ. Научно-производственный комплекс «Электрооборудование и системы управления для атомных электростанций» (НПК ЭАЭ). – URL: http://www.vniiem.orc.ru/atom_expro.htm. – (Дата обращения: 23.05.2016).
2. Компьютерный комплекс специального назначения ЭКСПРО: [Электронный ресурс]: АО «Корпорация «ВНИИЭМ» Электрооборудование и системы управления для АЭС. – URL: http://www.vniiem.ru/ru/index.php?option=com_content&view=article&id=126:2008-05-24-20-57-56&catid=38:npp&Itemid=63. – (Дата обращения: 23.05.2016).
3. Геча В. Я., Саранцев П. В., Козлов С. А. Разработка операционной системы Linem для информатизационно-диагностического комплекса электрооборудования управления защиты АЭС с реакторами типа ВВЭР-1000 // Электротехника. – 2004. – № 11. – С. 53 – 55.
4. Семенцов С. Г., Выпов П. А., Козлов С. А. Опыт создания специализированной операционной системы LiNem для систем управления и защиты АЭС // Вопросы электромеханики. Труды НПП ВНИИЭМ. – 2004. – Т. 101.
5. Герман Н. Р., Коноплев А. М. Опыт реализации подсистемы контроля и диагностики в составе операционной системы LiNem // Вопросы электромеханики. Труды НПП ВНИИЭМ. – 2004. – Т. 101.
6. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. Quality control of software systems. General principles. Дата введения 01.07.90. Меж-

государственный стандарт. – М.: ИПК Издательство стандартов. Источники: [Электронный ресурс]: Помощь по ГОСТам. – URL: <http://www.gosthelp.ru/text/GOST2819589Ocenkakachestv.html>. – (Дата обращения 23.05.2016); [Электронный ресурс]: Юридическая фирма Интернет и Право. – URL: <http://www.internet-law.ru/gosts/gost/11212/>. – (Дата обращения 23.05.2016).

7. Галеев А. П., Королёва В. А., Осипов Ю. В. Подход к расчёту надёжности информационных систем // Материалы Международного научно-методического семинара «Шумовые и деградационные процессы в полупроводниковых приборах», Москва, МНТОРЭС им. А. С. Попова, 28 – 30 ноября 2006 г. – М.: Изд-во МНТОРЭС им. А. С. Попова, 2006.

8. Майоров А. А., Соловьев И. В. Проектирование информационных систем / А. А. Майоров, И. В. Соловьёв. – М.: Академический проект, 2009. – 398 с.

9. Поляков А. А., Цветков В. Я. Прикладная информатика: учебно-методическое пособие для студентов вузов в двух частях / Под общей редакцией А. Н. Тихонова. – М.: Изд-во «МАКС Пресс», 2008. – Ч. 2. – 859 с.

10. Цветков В. Я. Стандартизация информационных программных средств и программных продуктов. – М.: МГУГиК, 2000. – 116 с.

11. Розенберг И. Н., Цветков В. Я. Информационные транзакционные затраты // Международный журнал прикладных и фундаментальных исследований. – 2010. – № 12. – С. 160 – 161.

12. Tsvetkov V. Ya. Dichotomous Systemic Analysis // Life Science Journal. – 2014. – 11(6). – P. 586 – 590.

13. Tsvetkov V. Ya. Information Constructions // European Journal of Technology and Design. – 2014. – Vol. 5(3). – P. 147 – 152.

14. Tsvetkov V. Ya. Information interaction // European Researcher. – 2013. – Vol. 62. – № 11 – 1. – P. 2573 – 2577.

15. Цветков В. Я. Формальная и содержательная классификация // Современные наукоёмкие технологии. – 2008. – № 6. – С. 85 – 86.

16. Цветков В. Я. Информационные модели объектов, процессов и ситуаций // Дистанционное и виртуальное обучение. – 2014. – № 5. – С. 4 – 11.

17. Монахов С. В., Савиных В. П., Цветков В. Я. Анализ прикладных систем / С. В. Монахов и др. – М.: Изд-во «МАКС Пресс», 2004. – 57 с.

18. Цветков В. Я. Развитие комплексной автоматизации производства. – М.: ГКНТ, ВНИИЦентр, 1988. – 100 с.

Поступила в редакцию 23.08.2016.

*Андрей Петрович Галеев, доцент, к.т.н., профессор, ст. научн. сотрудник,
т. (915) 207-50-34; e-mail: argal@inbox.ru.*

*Александр Алексеевич Майоров, д.т.н., профессор, зав. кафедры,
т. (499) 322-78-00; e-mail: portal@miigaik.ru.*

Московский государственный университет геодезии и картографии (МИИГАиК).

*Станислав Григорьевич Семенов, д.т.н., профессор,
т. (915) 001-89-86; e-mail: siemens_off@mail.ru.*

МГТУ им. Н.Э. Баумана.

*Владимир Тимофеевич Семёнов, начальник лаборатории,
т. (495) 366-38-38; e-mail: lab188@mcc.vniiem.ru.*

АО «Корпорация «ВНИИЭМ».

RELIABILITY EVALUATION of INFORMATION and DIAGNOSTIC COMPLEX

A.P. Galeev, A.A. Maiorov, S.G. Sementsov, V.T. Semionov

In the article, implementation of reliability evaluation method, used for information processing and representation at nuclear power plants, has been demonstrated by the example of the special purpose complex EXPRO (commercial version). The method includes reliability evaluation of equipment, testing and evaluation of software trouble-free operation. A procedure for complex hardware testing has been offered for consideration. Reliability block-diagram of the complex has been offered for consideration. Reliability calculation, including reliability calculations for software and hardware of the complex, has been performed. Statistic model for reliability function depending on complex operating time has been created. The article demonstrates that calculated reliability meets specified requirements for the whole operating period of complex.

Key words: software reliability, software hardware complex, backup, system software, reliability calculation.

List of References

1. Special purpose computer complex EXPRO: [Digital resource]: SPE VNIIEМ. Scientific and Production Complex «Electrical equipment and control systems for nuclear power plants» (SPC NPP EE). – URL: http://www.vniiem.org.ru/atom_expro.htm. – (Accessed date: 23.05.2016).
2. Special purpose computer complex EXPRO: [Digital resource]: SPE VNIIEМ. Scientific and Production Complex «Electrical equipment and control systems for nuclear power plants». – URL: http://www.vniiem.ru/ru/index.php?option=com_content&view=article&id=126:2008-05-24-20-57-56&catid=38:npp&Itemid=63. – (Accessed date: 23.05.2016).

3. Gecha V. Ia., Sarantsev P. V., Kozlov S. A. Developing of operational system Linem for Control and Protection System Electrical Equipment for NPP with Reactors WWER-1000 // *Electrotehnika*. – 2004. – No. 11. – Pp. 53 – 55.
4. Sementsov S. G., Vypov P. A., Kozlov S. A., Experience in creation of special purpose LiNem operating system for NPP control and protection systems // 2004. – Vol. 101.
5. German N. R., Konoplev A. M., Implementation experience of control and diagnostic subsystems of the LiNem operating system // *Issues of Electromechanics. VNIEM Works*. – 2004. – Vol. 101.
6. GOST 28195-89. Software quality evaluation. General provisions. Quality control of software systems. General principles. Effective date 01.07.90. Interstate standard. – M. : IPK Izdatelstvo standartov / Sources: [Digital resource]: Pomoshch po GOSTam [«Pomoshch po GOSTam» means website «gosthelp.ru» providing GOST information]. – URL: <http://www.gosthelp.ru/text/GOST2819589Ocenkakachestv.html>. – (Accessed date 23.05.2016); [Digital resource]: Law firm Internet&Law. – URL : <http://www.internet-law.ru/gosts/gost/11212/>. – (Accessed date 23.05.2016).
7. Galeev A. P., Koroleva V. A., Osipov Iu. V. Approaches to reliability calculation for information systems // *Proceedings of the Workshop «Noise and degradation processes in semiconductor devices»*. Moscow, MNTORES named after A.S. Popov, November 28 through 30, 2006. – M. : Izdatelstvo MNTORES named after A. S. Popov [MNTORES – Russian Scientific and Technical Society of Radio-Engineering, Electronics and Telecommunication named after A.S. Popov]. – 2006.
8. Maiorov A. A., Solovev I. V., Designing of Information systems / A. A. Maiorov, I. V. Solovev. – M. : Akademicheskii proect, 2009. – 398 pages.
9. Poliakov A. A., Tsvetkov V. Ia., Computer applications: study guide in two parts for college and university students / Under the general editorship of A. N. Tikhonov. – M. : Izdatelstvo «MAKS Press», 2008. – Part 2. – 859 pages.
10. Tsvetkov V. Ia., Software and software products standardization. – M. : MGUGiK [Moscow State University of Geodesy and Cartography (MIIGAiK)], 2000. – 116 pages.
11. Rozenberg I. N., Tsvetkov V. Ia., Information transaction costs // *International journal of applied and fundamental research*. – 2010. – No. 12. – Pp. 160 – 161.
12. Tsvetkov V. Ya. Dichotomous Systemic Analysis // *Life Science Journal*. – 2014. – 11(6). – P. 586 – 590.
13. Tsvetkov V. Ya. Information Constructions // *European Journal of Technology and Design*. – 2014. – Vol. 5(3). – P. 147 – 152.
14. Tsvetkov V. Ia. Information interaction // *European Researcher*. – 2013. Vol. 62 – No. 11 – 1. – Pp. 2573 – 2577.
15. Tsvetkov V. Ia., Form and content classification // *Modern knowledge intensive technologies*. – 2008. – No. 6. – Pp. 85 – 86.
16. Tsvetkov V. Ia. Information models of objects, processes and situations // *Remote and virtual learning*. – 2014. – No. 5. – Pp. 4 – 11.
17. Monakhov S. V., Savinykh V. P., Tsvetkov V. Ia., Applied systems analysis / S. V. Monakhov et al. – M. : Izdatelstvo «MAKS Press», 2004. – 57 pages.
18. Tsvetkov V. Ia. Development of complex manufacturing automation. – M. : GKNT, VNTITsentr, 1988. – 100 pages.

*Andrei Petrovich Galeev, Candidate of Technical Sciences (Ph. D.), Professor,
tel. (915) 207-50-34; e-mail: apgal@inbox.ru.*

*Aleksandr Alekseevich Maiorov, Doctor of Technical Sciences (D.Sc.), Professor, Chairman,
tel. (499) 322-78-00; e-mail: portal@miigaik.ru.
Moscow State University of Geodesy and Cartography (MIIGAiK).*

*Stanislav Grigorevich Sementsov, Doctor of Technical Sciences (D. Sc.),
tel. (915) 001-89-86; e-mail: siemens_off@mail.ru.
Bauman State Technical University.*

*Vladimir Timofeevich Semenov, Head of Laboratory,
tel. (495) 366-38-38; e-mail: lab188@mcc.vniem.ru.
JC «VNIEM Corporation».*