

МАРКОВСКИЕ МОДЕЛИ ГОТОВНОСТИ ВОССТАНАВЛИВАЕМЫХ STRATUS-СИСТЕМ

д.т.н., проф. В.С. Харченко, Ф.А. Асидех, к.т.н. И.В. Лысенко

Предложена классификация восстанавливаемых многоканальных дублированных архитектур (STRATUS-систем), исследован один из классов их марковских моделей надежности (готовности). Получены аналитические зависимости для коэффициента готовности для STRATUS-систем с произвольным числом подсистем.

Введение. Анализ проблемы отказоустойчивости бизнес-критических компьютерных систем (БКС). Известно, что развитие компьютерных систем и технологий идет очень быстро и требования к характеристикам их аппаратных и программных средств ужесточаются. Это объясняется как острой конкуренцией на рынке IT-технологий, так и динамичным расширением сферы их применения, ростом влияния на проблемы надежности и безопасности, поскольку компьютерные системы (КС) сейчас являются базовыми элементами сложных технических комплексов. Поэтому одно из важнейших требований к КС касается уровня их безотказности, готовности и отказоустойчивости и гарантоспособности в целом [1], особенно для критических и бизнес-критических приложений.

В последнее время к числу критических стали относить системы, используемые в биржевой и банковской деятельности, поскольку отказ и сбой в них приводят к большим денежным потерям. Ущерб от одного отказа компьютера в фирмах такого профиля по данным анализа 1000 фирм, проведенного департаментом финансов (Великобритания), составил 166 тыс. дол.; последствия отказа одного компьютера по данным фирмы FIND/SVP (США) в таких системах в среднем равны 263 тыс. дол. К числу системных решений и технологий, которые были ранее отработаны в критических приложениях, а затем развиты и используются в качестве коммерческих продуктов в БКС, относится технология STRATUS (фирма Hewlett Packard), основанная на отказоустойчивых мажоритарных и дублированных многоканальных архитектурах. Необходимо подчеркнуть, что системы с такими архитектурами используются в обслуживаемых БКС (которые, как правило, являются обслуживаемыми

мутатор; УУ – устройство управления; НРЧ – нерезервированная часть.

Признаками, по которым могут быть классифицированы STRATUS-системы, являются:

- тип модели восстановления работоспособности подсистемы;
- ресурс восстановления работоспособности устройств;
- тип стратегии восстановления работоспособности устройств.

Классификационная схема STRATUS-систем в соответствии с отмеченными признаками и стратегиями восстановления C_k представлена на рис. 2.

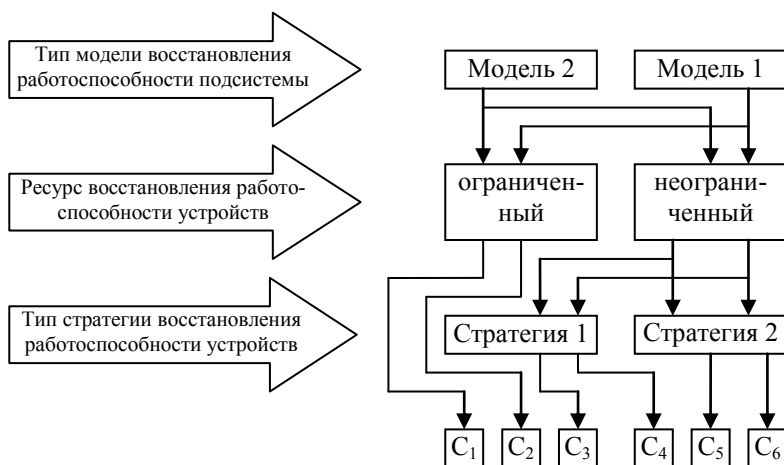


Рис. 2. Классификационная схема исследуемых STRATUS-систем

Методика исследования. Общая характеристика моделей. Методика исследования STRATUS-систем включает в себя следующие элементы:

- обоснование допущений и выбора показателя для оценки надежности STRATUS-систем, а также последовательности его расчета;
- обоснование выбора значений параметров системы;
- формирование множества вариантов (типов) исследуемых STRATUS-систем.

В основу разрабатываемых математических моделей надежности обслуживаемых компьютерных систем со STRATUS-архитектурой положены следующие допущения:

- процесс функционирования системы – марковский, т.е. потоки отказов и восстановлений работоспособности устройств системы стационарные пуассоновские с параметрами λ и μ ;

– ресурс восстановления работоспособности системы может быть ограниченным (одна ремонтная бригада, которая одновременно может выполнять мероприятия по восстановлению работоспособности только одного устройства системы) и неограниченным (имеется возможность привлечения необходимого числа ремонтных бригад для одновременного восстановления работоспособности нескольких отказавших устройств системы). В последнем случае процесс восстановления работоспособности системы может быть организован таким образом, что приоритет в восстановлении принадлежит устройствам, отказ которых приводит к отказу всей системы (стратегия 1 восстановления работоспособности), а также когда одновременно могут восстанавливаться устройства, отказ одних из которых приводит, а других не приводит к отказу системы;

– состояния системы S_i ($i = 1, \dots, n$), обусловленные отказами ее подсистем, могут быть представлены как аккумулирующие в себе обе причины отказа подсистемы, т.е. отказ одного из каналов – аппаратной компоненты (АК), либо программной компоненты (ПК) (модель 1 восстановления работоспособности подсистемы), а также состояния подсистемы, характеризующие отказ ее подсистем, могут дать дифференцированные с точки зрения причины отказа подсистемы, т.е. состояния S_i ($i = 1, \dots, n$), характеризующие отказ системы по причине отказа АК, и состояния S_j ($j = n + 1, \dots, 2n$) – по причине отказа ПК (модель 2 восстановления работоспособности подсистемы). При этом в первом случае (т.е. для модели 1) переход из состояния S_i в S_{i+1} осуществляется с интенсивностью $(n - i)\lambda + \lambda_{ПК}$, где λ – интенсивность отказов подсистемы, которая, в свою очередь, равна $\lambda = 2\lambda_{АК} + \lambda_{Н}$, где $\lambda_{Н}$ – интенсивность отказов нерезервированной части (НРЧ) подсистемы. Переход же из состояния S_{i+1} в S_i осуществляется с интенсивностью, зависящей от некоторой усредненной интенсивности восстановления подсистемы μ , где $\mu = (\mu_{АК} + \mu_{ПК} + \mu_{Н}) / 3$, а $\mu_{АК}$, $\mu_{ПК}$, $\mu_{Н}$ – интенсивность восстановления АК, ПК и НРЧ соответственно.

Для модели 2 $\forall I = 0, \dots, n$ переход из состояния S_{i+1} в S_i осуществляется с интенсивностью $\lambda_{ПК}$, а переходы $S_{n+1} \rightarrow S_i \forall I = 0, \dots, n - 1$ с интенсивностью $\mu_{ПК}$.

Наиболее полно надежность резервированных восстанавливаемых систем характеризуется коэффициентом готовности, представляющим собой вероятность события, состоящего в том, что система будет работоспособна в произвольный момент времени за исключением перехода времени ее планового технического обслуживания или ремонта. Как отмечается в [4, 5], получение выражения для расчета коэффициента го-

товности резервированных восстанавливаемых систем может быть осуществлено, минуя этап составления и решения системы однородных линейных алгебраических уравнений, а непосредственно из самого графа состояний в соответствии со следующим правилом: для определения стационарной вероятности P_i состояния S_i , необходимо идти по направлению стрелок из каждого крайнего состояния в i -е по кратчайшему пути и перемножить все интенсивности переходов, соответствующие всем переходимым стрелкам. Вообще же при “разветвленной” схеме состояний некоторые участки пути приходится проходить несколько раз, при этом интенсивности переходов этих участков нужно учитывать только

один раз. Тогда $P_i = \Pi_i / \sum_{j=0}^n \Pi_j$, где Π_i , Π_j – произведение интенсивно-

стей переходов из всех крайних состояний в i -е и j -е при движении по кратчайшему пути в направлении стрелок.

Если обозначить M_c , M_{pc} – множество всех и множество работоспособных состояний системы ($M_c \subset M_{pc}$) соответственно, а $|M_c|$, $|M_{pc}|$ – мощности этих множеств, то с учетом того, что стационарный коэффициент готовности есть сумма вероятностей P_i таких состояний S_i , что $S_i \in M_{pc}$, выражение для его вычисления в соответствии с вышеприведенной методикой может быть записано в виде

$$K_{\Gamma} = \frac{\sum_{i=0}^{|M_{pc}|-1} \Pi_{S_i}}{\sum_{i=0}^{|M_c|-1} \Pi_{S_i}}. \quad (1)$$

Учитывая, что знаменатель данного выражения определяется формулой

$$\sum_{i=0}^{|M_c|-1} \Pi_{S_i} = \sum_{i=0}^{|M_{pc}|-1} \Pi_{S_i} + \sum_{i=|M_{pc}|}^{|M_c|-1} \Pi_{S_i},$$

окончательно можно записать

$$K_{\Gamma} = \left[1 + \sum_{i=|M_{pc}|}^{|M_c|-1} \right]^{-1}. \quad (2)$$

Таким образом, коэффициент готовности системы будет являться

функцией интенсивностей отказов и восстановлений ее устройств.

В свою очередь, задание количественных значений параметров потоков отказов и восстановлений устройств STRATUS-систем целесообразно осуществлять таким образом, чтобы зафиксировать диапазон изменения значений некоторого базового параметра, а значения остальных выражать через значения этого базового параметра посредством коэффициентов, выражающих количественно соотношения между ними.

Исходные данные для исследования. Для интенсивности отказов выберем в качестве базового параметра *интенсивность отказов канала подсистемы* λ_{AK} со значениями $0,5 \cdot 10^{-6}$, 10^{-7} , $0,5 \cdot 10^{-7}$ 1/час.

Значения интенсивности отказов остальных устройств системы определим следующим образом:

- интенсивность отказов нерезервированной части подсистемы $\lambda_H = h\lambda_{AK}$, $h = 0,25; 0,5$;
- интенсивность отказов коммутатора $\lambda_{KM} = 0,1\lambda_{AK}$;
- интенсивность отказов устройства управления $\lambda_{УУ} = 0,1\lambda_{AK}$;
- интенсивность отказов программной компоненты $\lambda_{ПК} = \alpha\lambda_{AK}$, $\alpha = 1; 5; 10$.

В качестве базового параметра для интенсивности восстановления также примем *интенсивность восстановления канала подсистемы* μ_{AK} , т.е. интенсивность восстановления аппаратной компоненты.

Соотношение между $\mu_{ПК}$ и интенсивностями восстановления других устройств системы определим следующим образом:

- интенсивность восстановления нерезервированной части подсистемы $\mu_H = \mu_{AK}$;
- интенсивность восстановления коммутатора и устройства управления $\mu_{KM} = \mu_{УУ} = f\mu_{AK}$, $f = 1; 2$.

Что касается соотношения между μ_{AK} и $\mu_{ПК}$, будем исходить из следующего соображения: $\mu_{AK} = \mu_{ПК} = \mu$.

Математические модели восстанавливаемых STRATUS-систем. В качестве примера рассмотрим STRATUS-систему при ограниченном ресурсе восстановления работоспособности для модели 1 восстановления работоспособности (STRATUS-систем типа S_1 на рис. 2).

В соответствии с принятыми в модели 1 допущениями граф состояний STRATUS-системы с числом подсистем $n = 2$ может быть изображен следующим образом (рис. 3).

Интенсивность перехода из состояния S_0 в S_1 в данном случае равна $2\lambda + \lambda_{ПК}$, поскольку причиной перехода в состояние S_1 (одной работоспособной системы) может быть отказ любой из двух находящихся в

нагруженном режиме подсистемы или ПК. При этом интенсивность отказов подсистемы $\lambda = 2\lambda_{AK} + \lambda_H$, как было отмечено ранее. Таким образом, интенсивность перехода $S_0 \rightarrow S_1$ есть $2(2\lambda_{AK} + \lambda_H) + \lambda_{ПК} = 4\lambda_H + \lambda_{ПК}$ учитывая порядок величины $\lambda_{ПК}$, можно приближенно записать, что интенсивность перехода $S_0 \rightarrow S_1$ равна

$$2(\lambda + \lambda_{ПК}) = 2(2\lambda_{AK} + \lambda_H + \lambda_{ПК}) = 4\lambda_{AK} + 2\lambda_H + 2\lambda_{ПК}, \text{ т.е. } 2\lambda + \lambda_{ПК} \approx 2(\lambda + \lambda_{ПК}).$$

Данное допущение хотя и дает (практически неощутимое) заниженное значение рассчитанного в последствии значения коэффициента готовности системы, однако, позволяет существенно упростить получение отношений для его вычисления в соответствии с описанной методикой. Как следует из рис. 3, $|M_c| = 7$, $|M_{pc}| = 2$, тогда в соответствии с выражением (2) коэффициент готовности определяется из соотношения

$$K_{\Gamma} = \left[1 + \frac{\sum_{i=2}^6 \Pi_{S_i}}{\sum_{i=0}^1 \Pi_{S_i}} \right]^{-1}. \quad (3)$$

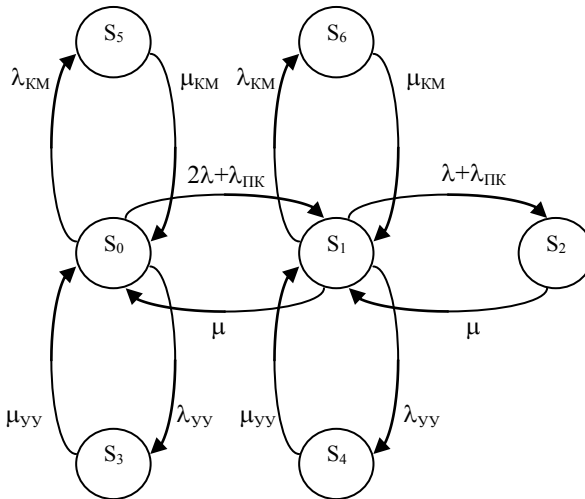


Рис. 3. Граф состояний для STRATUS-системы типа S1 при $n = 2$
В соответствии с вышеописанным правилом можно записать

$$K_{\Gamma} = \left[1 + \frac{\lambda_{yy}}{\mu_{yy}} + \frac{\lambda_{KM}}{\mu_{KM}} + \frac{2\lambda_1^2}{\mu^2 + 2\lambda_1\mu} \right]^{-1}. \quad (4)$$

После соответствующего преобразования последнего слагаемого

данное соотношение также можно записать в виде

$$K_{\Gamma} = \left[1 + \frac{\lambda_{yy}}{\mu_{yy}} + \frac{\lambda_{KM}}{\mu_{KM}} + \left[\frac{\mu}{\lambda_1} + \frac{\mu^2}{\mu^2 + 2\lambda_1^2} \right]^{-1} \right]^{-1}. \quad (5)$$

Для системы с $n = 3$ подсистемами граф состояний представлен на рис. 4. Действуя по аналогии, как при $n = 2$, т.е. определяя величины Π_{S_i} ($i = 0, \dots, 9$) и подставляя их в формулу для определения коэффициента готовности

$$K_{\Gamma} = \left[1 + \frac{\sum_{i=3}^9 \Pi_{S_i}}{\sum_{i=0}^2 \Pi_{S_i}} \right]^{-1}, \quad (6)$$

получим следующее соотношение

$$K_{\Gamma} = \left[1 + \frac{\lambda_{yy}}{\mu_{yy}} + \frac{\lambda_{KM}}{\mu_{KM}} + \frac{6\lambda_1^3}{\mu^3 + 3\lambda_1\mu^2 + 6\lambda_1^2\mu} \right]^{-1}. \quad (7)$$

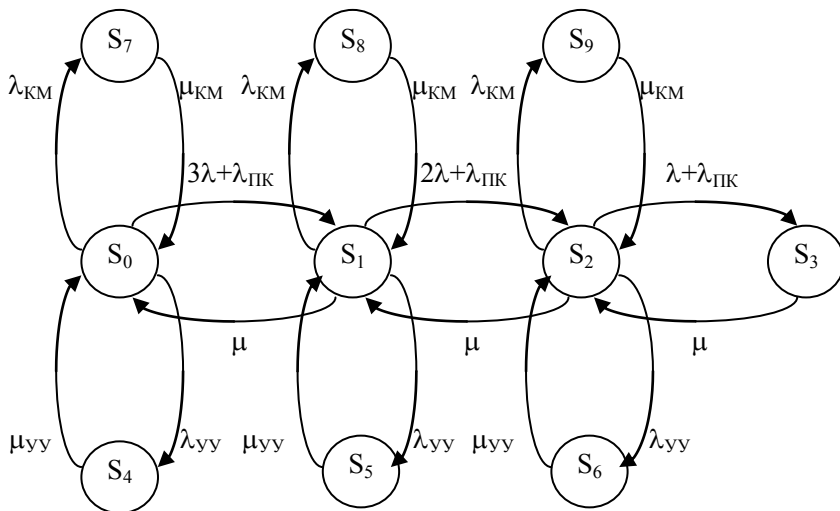


Рис. 4. Граф состояний для STRATUS-системы типа S_1 при $n = 3$
 Данное выражение также можно представить в виде

$$K_{\Gamma} = \left[1 + \frac{\lambda_{\text{УУ}}}{\mu_{\text{УУ}}} + \frac{\lambda_{\text{КМ}}}{\mu_{\text{КМ}}} + \left[\frac{\mu}{\lambda_1} + \frac{\mu^2}{2\lambda_1^2} + \frac{\mu^3}{6\lambda_1^3} \right]^{-1} \right]^{-1}. \quad (8)$$

Анализируя выражения (6) и (8), можно увидеть закономерность, которая позволяет записать обобщенное выражение для коэффициента готовности системы данного типа при произвольном значении n , т.е.

$$K_{\Gamma} = \left[1 + \frac{\lambda_{\text{УУ}}}{\mu_{\text{УУ}}} + \frac{\lambda_{\text{КМ}}}{\mu_{\text{КМ}}} + \left[\sum_{i=1}^n \frac{1}{i!} \left(\frac{\mu}{\lambda_1} \right)^i \right]^{-1} \right]^{-1}. \quad (9)$$

Значения коэффициента готовности системы (при $h = 0,25$ и $f = 1$) представлены в табл. 1.

Таблица 1

Значения коэффициента готовности системы

μ , 1/час	$\lambda_{\text{АК}} = 10^{-4}$ 1/час					
	$\alpha = 1$		$\alpha = 5$		$\alpha = 10$	
	$n = 2$	$n = 3$	$n = 2$	$n = 3$	$n = 2$	$n = 3$
0,1	0,999779	0,99980	0,999696	0,999798	0,999507	0,999789
0,5	0,999959	0,999960	0,999956	0,999960	0,999948	0,999960
1	0,999980	0,999980	0,999979	0,999980	0,999977	0,999980

μ , 1/час	$\lambda_{\text{АК}} = 10^{-6}$ 1/час					
	$\alpha = 1$		$\alpha = 5$		$\alpha = 10$	
	$n = 2$	$n = 3$	$n = 2$	$n = 3$	$n = 2$	$n = 3$
0,1	0,999998	0,999998	0,999998	0,999998	0,999998	0,999999
0,5	0,999999	0,999999	0,999999	0,999999	0,999999	0,999999
1	0,999999	0,999999	0,999999	0,999999	0,999999	0,999999

μ , 1/час	$\lambda_{\text{АК}} = 5 \cdot 10^{-7}$ 1/час					
	$\alpha = 1$		$\alpha = 5$		$\alpha = 10$	
	$n = 2$	$n = 3$	$n = 2$	$n = 3$	$n = 2$	$n = 3$
0,1	0,999999	0,999999	0,999999	0,999999	0,999999	0,999999
0,5	0,999999	0,999999	0,999999	0,999999	0,999999	0,999999
1	0,999999	0,999999	0,999999	0,999999	0,999999	0,999999

Анализ табл. 1 показывает:

а) для значений интенсивности отказов АК $\lambda_{\text{АК}}$, меньших 10^{-4} 1/час,

величина коэффициента готовности системы остается неизменной для различных комбинаций значений коэффициентов, выражающих соотношение между λ -характеристиками и характеристиками восстановления АК и других устройств системы, а также программной компоненты;

б) при $\lambda_{\text{АК}} = 10^{-4}$ 1/час величина относительного выигрыша по коэффициенту готовности STRATUS-системы с числом подсистем $n = 3$ по сравнению со STRATUS-системой при $n = 2$ и $\alpha = 10$ в среднем составляет 0,003%, а при $\alpha = 5$ – 0,001%, что свидетельствует об отсутствии необходимости увеличения кратности резервирования STRATUS-системы даже при относительно невысоких значениях $\lambda_{\text{АК}}$;

в) увеличение значения коэффициента f в 2 и 5 раз по сравнению с $f = 1$ дает величину относительного выигрыша по коэффициенту готовности в среднем на 0,001 и 0,016% соответственно при $\lambda_{\text{АК}} = 10^{-4}$ 1/час.

Выводы. Сравнительный анализ результатов исследования рассмотренных STRATUS-систем показывает, что:

а) наибольшим значением интенсивности отказов аппаратной компоненты системы, при котором величина коэффициента готовности системы остается неизменной для различных комбинаций значений коэффициентов, выражающих соотношение между λ -характеристиками и характеристиками восстановления АК и других устройств системы, а также программной компоненты, является $\lambda_{\text{АК}} = 10^{-4}$ 1/час. Данное обстоятельство является подтверждением факта высокой надежности системы;

б) при $\lambda_{\text{АК}} = 10^{-4}$ 1/час значения коэффициента готовности (при неограниченном ресурсе восстановления как для модели 1, так и модели 2 для заданного диапазона значений параметров h, f, μ, α) при стратегии 2 превышает значения коэффициента готовности при стратегии 1 в среднем на $0,007 \div 0,01\%$. Для $n = 2$, а для $n = 3$ это превышение практически равно нулю (сравниваемые системы S_3 и S_5, S_4 и S_6);

в) увеличение значения интенсивности отказов подсистема μ в 5 и 10 раз по сравнению с $\mu = 1$ 1/час дает прирост значения коэффициента готовности STRATUS-систем рассматриваемых типов в среднем на 0,02% для $n = 2$ и 0,01% для $n = 3$;

г) при значении интенсивности отказов аппаратной компоненты $\lambda_{\text{АК}} = 10^{-6}$ 1/час прирост значений коэффициента готовности как для модели 1, так и модели 2 восстановления работоспособности подсистемы для STRATUS-систем с неограниченным ресурсом восстановления работоспособности по сравнению со STRATUS-системами с неограни-

ченным ресурсом восстановления работоспособности имеет место только при $\alpha \geq 100$ (т.е. когда интенсивность отказов программной компоненты минимум на 2 порядка превышает интенсивность отказов аппаратной компоненты системы).

Дальнейшие исследования целесообразно направить на разработку и анализ моделей многоверсионных обслуживаемых STRATUS-систем.

ЛИТЕРАТУРА

1. Avizienis Algirdas, Jean-Claude Laprie, Brian Randell. *Fundamental Concepts of Dependability* // *Technical Report: UCLA CSD Report no. 010028, LAAS Report no. 01-145, Newcastle University Report no. CS-TR-739. UCLA Computer Science Dept. Univ. of California, Los Angeles, USA; LAAS-CNRS, Toulouse, France; Dept. of Computing Science Univ. of Newcastle-upon-Tyne, U.K. 2002. – 19 p.*
2. Харченко В.С., Асидех Ф.А. Базовые архитектуры многоканальных дублированных систем, устойчивые к отказам аппаратных и программных средств // *Вестник технологического университета Подолья. – 2002. – № 3. – Том 1. – С. 55 – 59.*
3. Харченко В.С., Асидех Ф.А. Методы повышения отказоустойчивости бизнес-критических компьютерных систем с использованием многоверсионных STRATUS-технологий // *Сборник научных трудов национального аэрокосмического университета им. Н.Е. Жуковского “ХАИ” – 2002. – № 15. – С. 47 – 58.*
4. Харченко В.С., Харченко К.В. COTS- и CrOTS-подходы к повышению эффективности критических и коммерческих IT-проектов // *Системы обработки информации. – X.: НАНУ, ПАНМ, ХВУ. – 2002. – Вып. 2(18). – С. 252 – 258.*
5. Дружинин Г.В. и др. *Теория надежности радиоэлектронных систем в примерах и задачах. – М.: Энергия, 1976. – 259 с.*
6. Половко А.М. и др. *Сборник задач по теории надежности. – М.: Сов. радио, 1972. – 408 с.*

Поступила 2.02.2004

ХАРЧЕНКО Вячеслав Сергеевич, докт. техн. наук, профессор, зав. кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского “ХАИ”. В 1974 году окончил Харьковское высшее командно-инженерное училище ракетных войск. Область научных интересов — теоретические основы, методы проектирования и экспертизы компьютерных систем критического применения.

АСИДЕХ Фатхи Али, аспирант кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского “ХАИ”. В 2001 году окончил Национальный аэрокосмический университет им. Н.Е. Жуковского “ХАИ”. Область научных интересов — надежность и отказоустойчивость бизнес-критических компьютерных систем.

ЛЫСЕНКО Игорь Владимирович, канд. техн. наук, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского “ХАИ”. В 1992 году окончил Харьковский военный университет. Область научных интересов — методы моделирования и оценки надежности информационных и управля-

ющих систем.