УДК 62-192.001

В.С. ХАРЧЕНКО, В.В. СКЛЯР, О.М. ТАРАСЮК

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

БЕЗОПАСНОСТЬ АЭРОКОСМИЧЕСКОЙ ТЕХНИКИ И НАДЕЖНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Проведен анализ рисков, возникающих при использовании аэрокосмической (авиационной и ракетно-космической) техники (АРКТ) вследствие отказов их оборудования и различных системных компонент. Сопоставлены причины отказов авиационной (АТ) и ракетно-космической (РКТ) техники. Представлены результаты их эволюционного анализа для РКТ за последние сорок лет. Дана оценка влияния отказов компьютерных систем управления, их аппаратных и программных средств на аварии РКТ

безопасность авиационной и ракетно-космической техники, надежность компьютерных систем управления

Введение. Проблема анализа рисков аварий АРКТ

Развитие техники привело к созданию систем, которые несут в себе потенциальную угрозу природе и человеческому обществу [1]. Большая часть аварий и катастроф последних десятилетий носит техногенный характер. Из всех потенциальных техногенных источников нарушения глобальной безопасности наиболее значимыми являются АЭС и ракетоносители (РН), причем опасность представляют не только боевые РН, оснащенные ядерными боеголовками, но и «мирные», предназначенные для выполнения коммерческих и научно-исследовательских задач. Аварии самолетов военной и гражданской авиации исключительно опасны и сами по себе, и вследствие возможного поражения в результате этих аварий других критических объектов. При анализе таких систем важное место занимает анализ рисков [2, 3]. Понятие риска характеризуется неопределенностью, связанной с возможностью возникновения неблагоприятных ситуаций в ходе эксплуатации технических систем.

Авиационная и ракетно-космическая отрасли являются одними из важнейших секторов мировой экономики с многомиллиардными оборотами. Кроме того, исторически сложилось так, что прогресс человечества в целом принято оценивать в том числе и степенью развития авиации и космонавтики, а наличие и поддержание «аэрокосмического имиджа» во многом определяет авторитет государства в мировом сообществе. В то же время, положение дел в области безопасности авиационной и ракетно-космической техники оставляет желать лучшего. За вековую историю авиации и неполных полвека космической эры накоплена обширная статистика об отказах, авариях и катастрофах, изучение которой может дать весьма полезные результаты [4].

Мировое сообщество с трагической регулярностью будоражат известия об очередных авиационных катастрофах и авариях РН или космических аппаратов (КА). Такие события приводят к многомиллионным потерям, экологическим катастрофам, а в худшем случае – уносят человеческие жизни.

Целью данной статьи является проведение анализа рисков аварий, возникающих при использовании АРКТ вследствие отказов их оборудования и компьютерных систем. Данная статья расширяет результаты исследований, опубликованных в [5], которые дополнены сопоставительным анализом причин отказов АТ и РКТ, а также оценкой влияния на их безопасность ранее разработанного программного обеспечения.

1. Исходная информация, задачи и методология проведения исследования

Первоначальная задача, которую ставили перед собой авторы, была связана с эволюционным анализом влияния надежности компьютерных средств и систем на безопасность АРКТ. Однако затем по мере накопления материала границы этой задачи распространились и на другие системные компоненты, прежде всего для РКТ.

При подготовке материалов использовались доступные авторам открытые источники. При этом необходимо подчеркнуть, что систематизированные количественные данные о причинах отказов АТ, несмотря на более обширную выборку по сравнению с РКТ, практически отсутствуют. Это, очевидно, связано с закрытым характером такой информации [6 - 8]. Поэтому далее основное внимание уделено анализу аварий РКТ. Что касается АТ, то в статье на основе сложившейся в авиации таксономии [9] анализируются основные причины аварий в сопоставлении с РКТ.

В работе исследована статистика аварий ракетно-космической техники за 40 лет, с 1961 г. по 2000 г. включительно [4]. Приводимая информация может расходиться с другими источниками, так как до сих пор нет полностью достоверных данных о всех катастрофах. При проведении исследования не рассматривались данные по отказам и авариям баллистических и крылатых РН военного назначения.

На протяжении долгого времени история освоения космоса являлась историей противоборства между двумя сверхдержавами – СССР и США. Поэтому при исследовании статистические данные были сгруппированы в соответствии с их принадлежностью этим двум государствам. После 1991 г. преемником СССР стала Россия. В ряду нескольких аэрокосмических государств в мире, способных самостоятельно создавать самолеты, РН и КА, по праву находится Украина, предприятия которой непосредственно выполняют разработку и производство РН, систем управления и другой аппаратуры и активно участвуют в выполнении различных проектов совместно с Россией, США и другими странами. Что касается остальных государств, осуществлявших пуски ракет-носителей, то их вклад в освоение космоса выглядит гораздо более скромным (см. табл. 1), поэтому статистические данные для них не дифференцировались, а были объединены под названием «Другие страны». Исследование проводилось по следующим направлениям:

– анализ рисков для аварий РН;

– анализ рисков для аварий космических аппаратов (КА);

– анализ тенденций изменения рисков отказов различных составляющих РН и КА, в том числе аппаратных и программных средств БКС;

– анализ рисков для аварий АТ и их сравнение с РКТ.

Методология исследований базируется на системном анализе рисков аварий и катастроф по разным классификационным признакам и представлении результатов в виде диаграмм и трендов.

2. Анализ пусков ракетоносителей

Полные данные о количестве пусков ракетоносителей приведены в табл. 1. В ней учтены только пуски, зарегистрированные Комиссией ООН по исследованию и использованию космического пространства (COSPAR) и Космическим командованием США (NORAD). В данную таблицу включены только успешные пуски, то есть те, которые завершались выводом полезной нагрузки на орбиту.

3. Анализ рисков для аварий ракетоносителей

В табл. 2 приведены сводные данные по отказам РН, сгруппированные в соответствии со странами-разработчиками РН (СССР/Россия, США, другие страны и международные проекты Arianespace и Sea Launch).

Таблица 1

Запуски ракетоносителей в период 1959 - 2000 гг.

Год	СССР / Россия	США	Франция	Япония	Китай	Велико-британия	Индия	Израиль	Arianespace	Sea Launch	ВСЕГО
1959	3	11									14
1960	3	16									19
1961	6	29									35
1962	20	52									72
1963	17	38									55
1964	30	57									87
1965	48	63	1								112
1966	44	73	1								118
1967	66	59	2								127
1968	74	45									119
1969	70	40									110
1970	81	29	2	1	1						114
1971	83	32	1	2	1	1					120
1972	74	31		1							106
1973	86	23									109
1974	81	24		1							106
1975	89	28	3	2	3						125
1976	99	26		1	2						128
1977	98	24		2							124
1978	88	32		3	1						124
1979	87	16		2					1		106
1980	89	13		2			1				105
1981	98	18		3	1		1		2		123
1982	101	18		1	1						121
1983	98	22		3	1		1		2		127
1984	97	22		3	3				4		129
1985	98	17		2	1				3		121
1986	91	6		2	2				2		103
1987	95	8		3	2				2		110
1988	90	12		2	4			1	7		116
1989	74	18		2					7		101
1990	75	27		3	5			1	5		116
1991	59	18		2	1				8		88
1992	54	28		1	4		1		7		95
1993	47	23		1	1				7		79
1994	48	26		2	5		2		6		89
1995	32	27		1	2			1	11		74
1996	25	33		1	3		1		10		73
1997	28	37		2	6		1		12		86
1998	24	34		2	6				11		77
1999	26	30			4		1		10	2	73
2000	35	28			5				12	3	82
ВСЕГО	2634	1220	10	53	65	1	9	3	129	5	4128

Графическое отображение данных из табл. 2 представлено на рис. 1, 2.

Риски запуска РН (вероятность аварии) рассчитывались как отношение числа аварийных пусков $N_{\text{ав.РН}}$ к общему числу успешных $N_{\text{усп.РН}}$ и аварийных $N_{ав.\text{РН}}$ пусков по формуле:

$$Risk_{\text{РН}} = N_{\text{ав.РН}} / \left(N_{\text{усп.п}} + N_{\text{ав.РН}} \right). \quad (1)$$

Таблица 2

Анализ рисков для отказов ракетоносителей в период 1961 - 2000 гг.

Год	СССР/Россия			США			Другие страны			Всего		
	Кол-во успешных пусков	Кол-во аварий РН	Риск	Кол-во успешных пусков	Кол-во аварий РН	Риск	Кол-во успешных пусков	Кол-во аварий РН	Риск	Кол-во успешных пусков	Кол-во аварий РН	Риск
1961	6	3	0,333	29	13	0,31	0	0	−	35	16	0,314
1962	20	2	0,091	52	9	0,148	0	0	−	72	11	0,133
1963	17	7	0,292	38	8	0,174	0	0	−	55	15	0,214
1964	30	6	0,167	57	8	0,123	0	0	−	87	14	0,139
1965	48	6	0,111	63	8	0,113	1	0	0	112	14	0,111
1966	44	9	0,17	73	4	0,052	1	3	0,75	118	16	0,119
1967	66	11	0,143	59	3	0,048	2	3	0,6	127	17	0,118
1968	74	8	0,098	45	4	0,082	0	1	1	119	13	0,098
1969	70	14	0,167	40	1	0,024	0	1	1	110	16	0,127
1970	81	7	0,08	29	0	0	4	0	0	114	7	0,058
1971	83	9	0,098	32	3	0,086	5	2	0,286	120	14	0,104
1972	74	5	0,063	31	2	0,061	1	0	0	106	7	0,062
1973	86	4	0,044	23	2	0,08	0	2	1	109	8	0,068
1974	81	4	0,047	24	1	0,04	1	1	0,5	106	6	0,054
1975	89	4	0,043	28	4	0,125	8	0	0	125	8	0,06
1976	99	2	0,02	26	0	0	3	1	0,25	128	3	0,023
1977	98	3	0,03	24	3	0,111	2	0	0	124	6	0,046
1978	88	4	0,043	32	1	0,03	4	0	0	124	5	0,039
1979	87	0	0	16	0	0	3	2	0,4	106	2	0,019
1980	89	0	0	13	2	0,133	3	1	0,25	105	3	0,028
1981	98	0	0	18	1	0,053	7	0	0	123	1	0,008
1982	101	0	0	18	0	0	2	1	0,333	121	1	0,008
1983	98	0	0	22	0	0	7	0	0	127	0	0
1984	97	0	0	22	0	0	10	0	0	129	0	0
1985	98	0	0	17	1	0,056	6	1	0,143	121	2	0,016
1986	91	0	0	6	3	0,333	6	1	0,143	103	4	0,037
1987	95	1	0,01	8	1	0,111	7	1	0,125	110	3	0,027
1988	90	0	0	12	0	0	14	1	0,067	116	1	0,009
1989	74	0	0	18	0	0	9	1	0,1	101	1	0,01
1990	75	0	0	27	0	0	14	1	0,067	116	1	0,009
1991	59	0	0	18	1	0,053	11	0	0	88	1	0,011
1992	54	0	0	28	1	0,034	13	0	0	95	1	0,01
1993	47	0	0	23	2	0,08	9	1	0,1	79	3	0,037
1994	48	1	0,02	26	1	0,037	15	2	0,118	89	4	0,043
1995	32	0	0	27	5	0,156	15	2	0,118	74	7	0,086
1996	25	0	0	33	0	0	15	3	0,167	73	3	0,039
1997	28	3	0,097	37	1	0,026	21	1	0,045	86	5	0,055
1998	24	2	0,077	34	2	0,056	19	2	0,095	77	6	0,072
1999	26	2	0,071	30	6	0,167	17	2	0,105	73	10	0,12
2000	35	3	0,079	28	0	0	20	1	0,048	83	4	0,046

Средние значения рисков рассчитывались от общего количества пусков и аварий. Следует отметить, что количество аварий РН, как и численное значение риска аварии, и для России, и для США с самого начала освоения космоса имело стойкую тенденцию к снижению. Риск аварии РН снизился от 30% в начале 60-х годов до нулевого значения в середине 80-х.

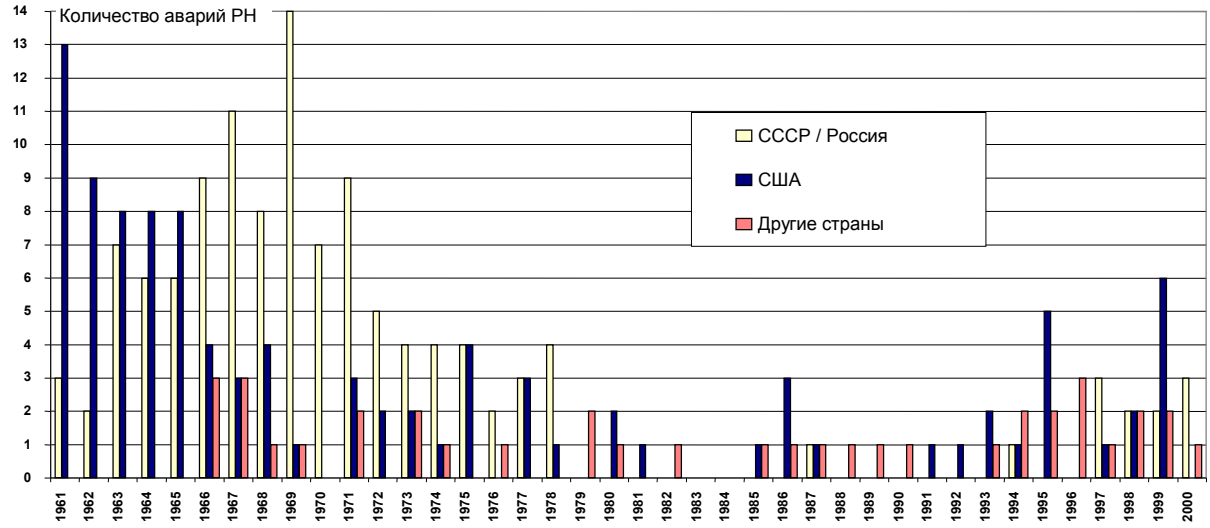


Рис. 1. Распределение аварий ракетоносителей между странами-изготовителями

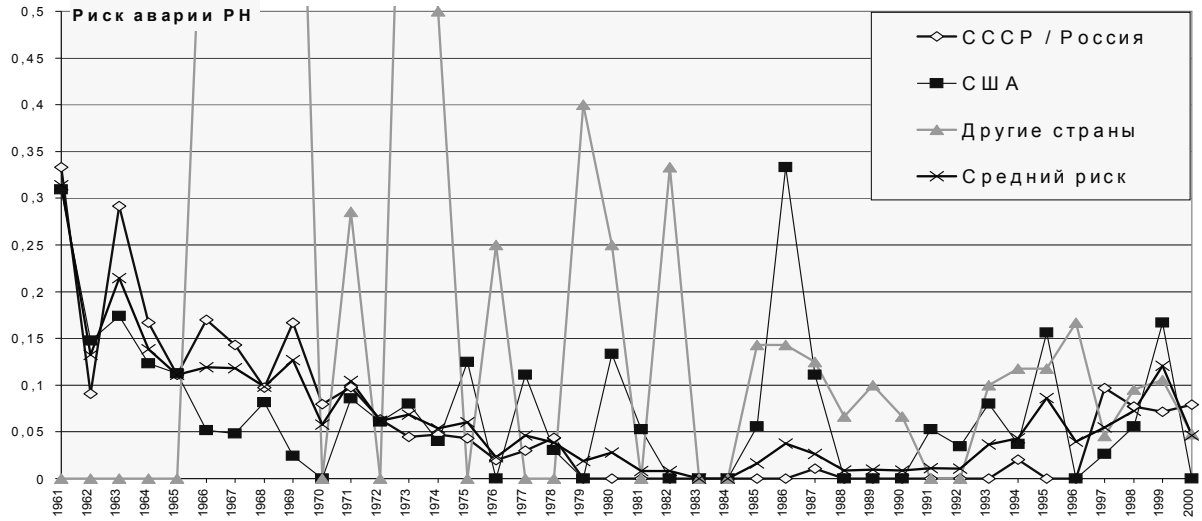


Рис. 2. Значения рисков аварий ракетоносителей

Остальные страны в то время несколько отставали в развитии РКТ от СССР и США. Количество пусков во всем остальном мире (исключая СССР и США) не превышало десятка в год, РН проходили этап приработки, поэтому значения рисков были весьма велики и отличались значительными флуктуациями. Со второй половины 80-х годов количество аварий РН и соответствующие риски опять возрастают. Это объясняется возросшим количеством коммерческих пусков, обусловленным бурным развитием телекоммуникационных технологий. Значения рисков имеют значительные флуктуации, но их максимальные значения не превосходят 0,167 (другие страны – 1995 г., США – 1999 г.). Среднее значение рисков во второй половине 90-х годов колеблется в диапазоне 0,05…0,10. Похоже, что данная тенденция приняла устойчивый характер и может сохраняться в ближайшие годы. Следовательно, фирмам, работающим в ракетно-космической отрасли, придется смириться с потерями от 5 до 10 ракет на каждые 100 пусков.

4. Анализ рисков для аварий космических аппаратов

В табл. 3 приведены сводные данные по отказам КА, сгруппированные в соответствии со странами-разработчиками РН (СССР/Россия, США, другие

страны). Риски аварии КА определялись из расчета на один успешный пуск:

$$Risk_{\text{КА}} = N_{\text{ав. КА}} / N_{\text{усп. п}}. \qquad (2)$$

Под успешным пуском КА здесь понимается его вывод на расчетную орбиту и эксплуатация в течение всего установленного срока службы.

Таблица 3

Анализ рисков для отказов космических аппаратов в период 1961 - 2000 гг.

Год	СССР/Россия			США			Другие страны			Всего		
	Кол-во успешных пусков	Кол-во аварий КА	Риск	Кол-во успешных пусков	Кол-во аварий КА	Риск	Кол-во успешных пусков	Кол-во аварий КА	Риск	Кол-во успешных пусков	Кол-во аварий КА	Риск
1961	6	1	0,167	29	1	0,034	0	0	–	35	2	0,057
1962	20	2	0,1	52	0	0	0	0	–	72	2	0,028
1963	17	3	0,176	38	0	0	0	0	–	55	3	0,055
1964	30	2	0,067	57	1	0,018	0	0	–	87	3	0,034
1965	48	8	0,167	63	1	0,016	1	0	0	112	9	0,08
1966	44	0	0	73	2	0,027	1	0	0	118	2	0,017
1967	66	2	0,03	59	1	0,017	2	0	0	127	3	0,024
1968	74	4	0,054	45	0	0	0	0	–	119	4	0,034
1969	70	3	0,043	40	0	0	0	1	–	110	4	0,036
1970	81	0	0	29	1	0,034	4	1	0,25	114	2	0,018
1971	83	5	0,06	32	1	0,031	5	0	0	120	6	0,05
1972	74	0	0	31	0	0	1	0	0	106	0	0
1973	86	3	0,035	23	2	0,087	0	0	–	109	5	0,046
1974	81	2	0,025	24	1	0,042	1	0	0	106	3	0,028
1975	89	2	0,022	28	0	0	8	0	0	125	2	0,016
1976	99	4	0,04	26	0	0	3	0	0	128	4	0,031
1977	98	4	0,041	24	2	0,083	2	0	0	124	6	0,048
1978	88	1	0,011	32	0	0	4	0	0	124	1	0,008
1979	87	0	0	16	0	0	3	0	0	106	0	0
1980	89	0	0	13	0	0	3	0	0	105	0	0
1981	98	0	0	18	0	0	7	0	0	123	0	0
1982	101	0	0	18	0	0	2	0	0	121	0	0
1983	98	0	0	22	0	0	7	0	0	127	0	0
1984	97	0	0	22	0	0	10	0	0	129	0	0
1985	98	0	0	17	0	0	6	0	0	121	0	0
1986	91	0	0	6	0	0	6	0	0	103	0	0
1987	95	1	0,011	8	0	0	7	0	0	110	1	0,009
1988	90		0	12	0	0	14	0	0	116	0	0
1989	74		0	18	0	0	9	0	0	101	0	0
1990	75		0	27	1	0,037	14	1	0,071	116	2	0,017
1991	59		0	18	1	0,056	11	1	0,091	88	2	0,023
1992	54		0	28	0	0	13	0	0	95	0	0
1993	47		0	23	0	0	9	0	0	79	0	0
1994	48		0	26	1	0,038	15	1	0,067	89	2	0,022
1995	32		0	27	2	0,074	15	1	0,067	74	3	0,041
1996	25		0	33	1	0,03	15	0	0	73	1	0,014
1997	28	7	0,25	37	2	0,054	21	3	0,143	86	12	0,14
1998	24	5	0,208	34	9	0,265	19	2	0,105	77	16	0,208
1999	26	3	0,115	30	7	0,233	17	2	0,118	73	12	0,164
2000	35		0	28	1	0,036	20	2	0,1	83	3	0,036

Визуальное отображение данных из табл. 3 представлено на рис. 3, 4.

В 60-е годы большее (по сравнению с США) число аварий происходило с советскими КА. Ситуация между СССР и США выровнялась в начале 70-х годов, а к концу 70-х годов аварии КА практически прекратились. Это объясняется тем, что технологии проектирования, изготовления и эксплуатации КА достигли к этому времени определенного совершенства, а наиболее сложные программы межпланетных полетов к Луне, Марсу, Венере были уже выполнены. Другие страны в это время эксплуатировали незначительное количество КА, поэтому как количество аварий, так и значения рисков КА для них имеют нулевое значение.

Возрастание количества аварий КА началось с 90-х годов и связано с развитием телекоммуникационных технологий, усложнением выполняемых задач и возрастанием требований к надежности работы и сроку службы КА. К концу 90-х годов значения рисков КА превысили показатели, характеризующие самое начало космической эры и превысили значение 25%. Соответственно, каждый четвертый КА «не доживает» до конца запланированного срока эксплуатации. Разумеется, этот факт не может не тревожить разработчиков и заказчиков, так как цена таких отказов крайне велика.

На рис. 5, 6 проведен сравнительный анализ количества аварий и значений рисков для РН и КА. На рис. 6, кроме средних значений рисков аварий КА и РН, добавлено значение суммарного риска выполнения задачи КА, составляющими которого являются риск аварии КА и риск аварии РН. Получим формулу для определения риска выполнения задачи КА. Вероятность выполнения задачи:

$$P_{\text{Вып.з}} = 1 - Risk_{\text{Вып.з}}. \quad (3)$$

В то же время

$$P_{\text{Вып.з}} = P_{\text{РН}} P_{\text{КА}} = (1 - Risk_{\text{РН}})(1 - Risk_{\text{КА}}). \quad (4)$$

Отсюда

$$1 - Risk_{\text{Вып.з}} = (1 - Risk_{\text{РН}})(1 - Risk_{\text{КА}}) \quad (5),$$

и окончательно

$$Risk_{\text{Вып.з}} = Risk_{\text{РН}} + Risk_{\text{КА}} - Risk_{\text{РН}} Risk_{\text{КА}}. \quad (6)$$

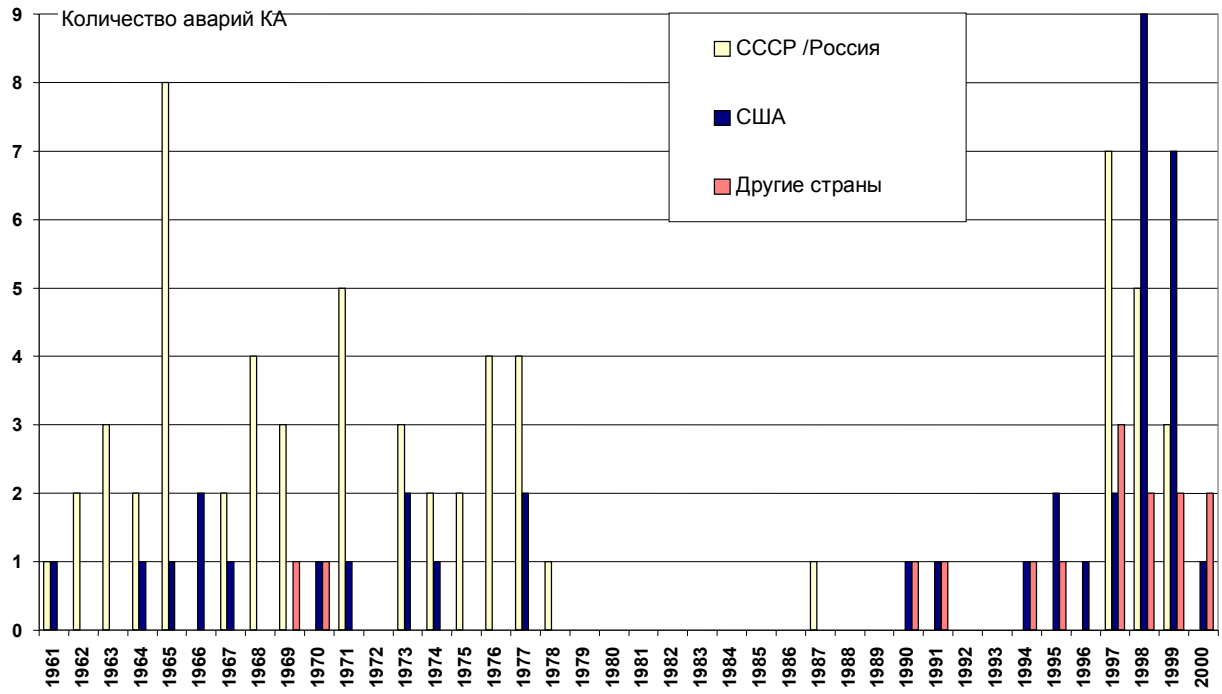


Рис. 3. Распределение аварий космических аппаратов между странами-изготовителями

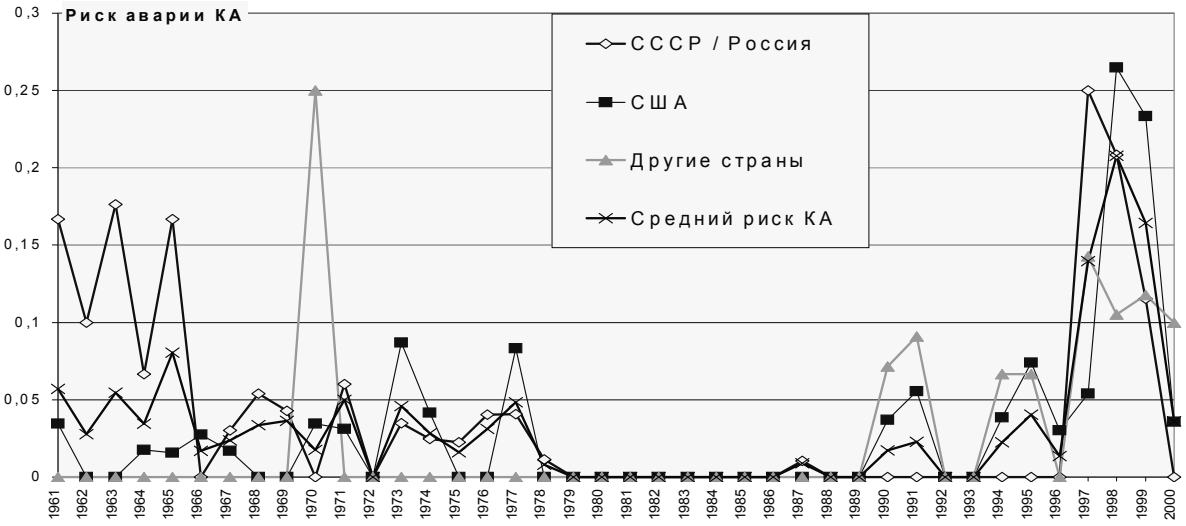


Рис. 4. Значения рисков аварий космических аппаратов

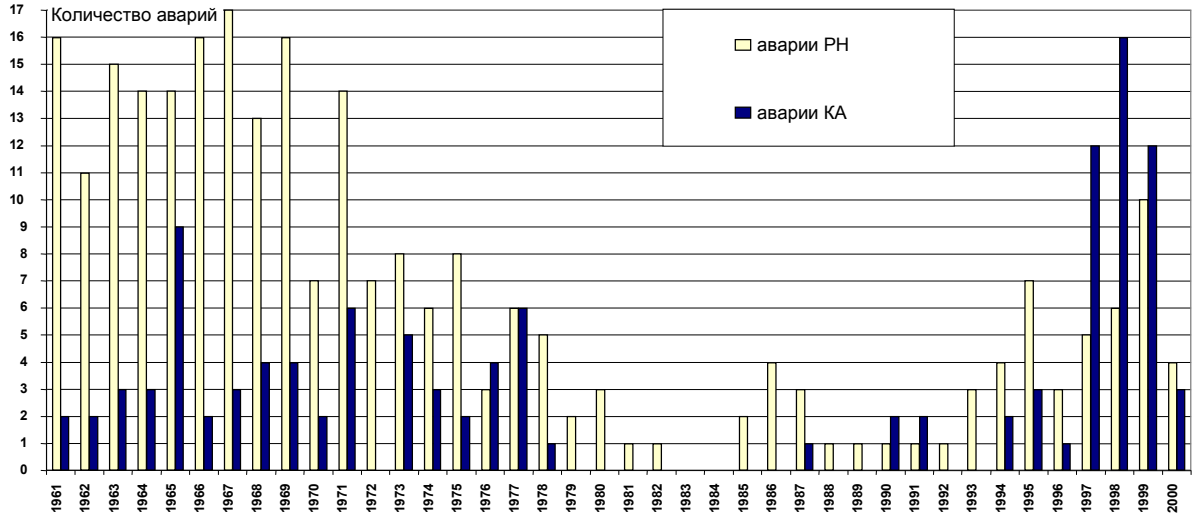


Рис. 5. Сравнительный анализ количества аварий ракетоносителей и космических аппаратов

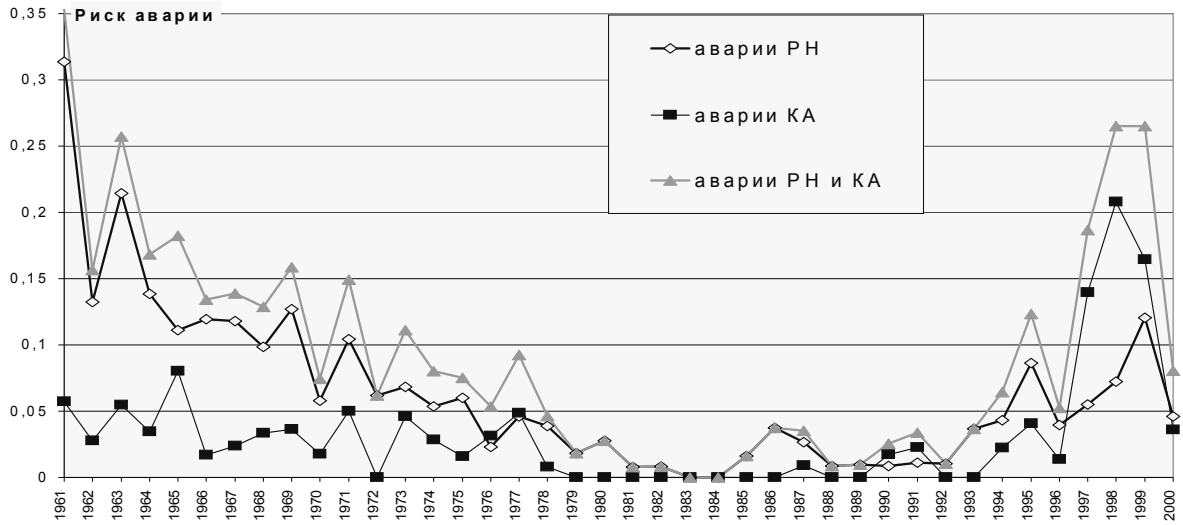


Рис. 6. Сравнительный анализ значений рисков аварий ракетоносителей и космических аппаратов

Проведенный анализ показал, что до середины 70-х годов риск аварий РН в два и более раз превосходил риск аварий КА. Затем значения этих рисков приблизительно выровнялись, а со второй половины 90-х годов риски аварий КА превзошли риски аварий РН. Таким образом, на современном этапе развития РКТ наиболее «узким» местом выполнения возложенной на КА миссии является не его доставка на орбиту, а обеспечение безотказной работы КА в течение запланированного срока эксплуатации.

5. Анализ тенденций изменения рисков аварий из-за отказов различных составляющих РН и КА

В табл. 4 исследована динамика изменения процентного соотношения отказов, приведших к авариям РН и КА. Расчеты проводились для временных интервалов длительностью 10 лет. Отдельно выделен ряд причин отказов, общих для РН и КА. Следует отметить, что для 60 - 80-х годов из-за недостатка информации не произведена дифференциация отказов для КА. Результаты анализа данных табл. 4 представлены на рис. 7 - 11. Для определения риска аварии из-за отказа той или иной составляющей в ходе выполнения космического полета необходимо воспользоваться формулой

$$Risk_i = N_{\text{аварий } i} / \left(N_{\text{усп. п}} + N_{\text{аварий РН}} \right). \qquad (7)$$

Риски аварий из-за отказов составляющих РКТ, отражающие современные тенденции, приведены в табл. 5 (рассчитаны на основе статистики за 90-е годы). При этом учтено, что в 90-х годах было осуществлено 816 успешных пусков и произошло 44 аварии РН (см. табл. 1, 2).

Таблица 4

Причины отказов РКТ

Причины аварий	60-е годы		70-е годы		80-е годы		90-е годы	
	кол-во	%	кол-во	%	кол-во	%	кол-во	%
Отказы и взрывы ступеней ракетоносителя (РН)	136	79	60	66	38	90	31	29
Отказы космических аппаратов (КА)	9	5	9	10	0	0	0	0
Отказы двигательных установок (ДУ)	6	3	5	5	1	2,5	10	10
Отказы радиоаппаратуры (РА)	2	1	2	2	1	2,5	7	7
Отказы разгонных блоков (РБ)	3	2	1	1	1	2,5	6	6
Отказы систем электропитания и кабельных сетей (СЭП)	2	1	1	1	0	0	9	9
Отказы систем управления (СУ)	16	9	14	15	1	2,5	24	23
Отказы аппаратных средств бортовых компьютеров (АС)	0	0	0	0	0	0	6	6
Отказы программных средств бортовых компьютеров (ПС)	0	0	0	0	0	0	10	10
ВСЕГО	174	–	92	–	42	–	103	–

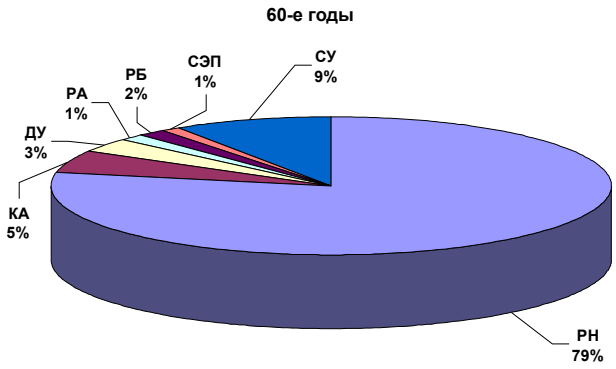


Рис. 7. Распределение причин отказов ракетно-космической техники в 60-е годы

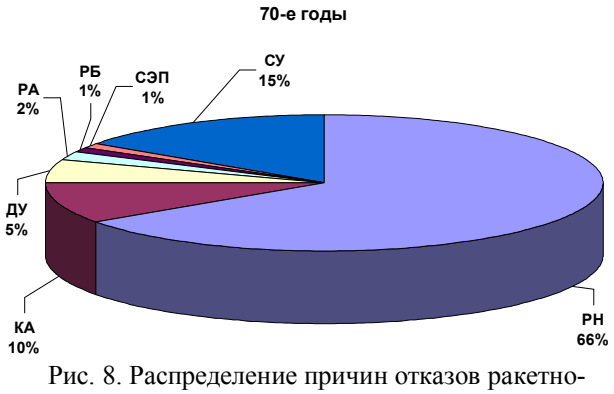


Рис. 8. Распределение причин отказов ракетно-космической техники в 70-е годы

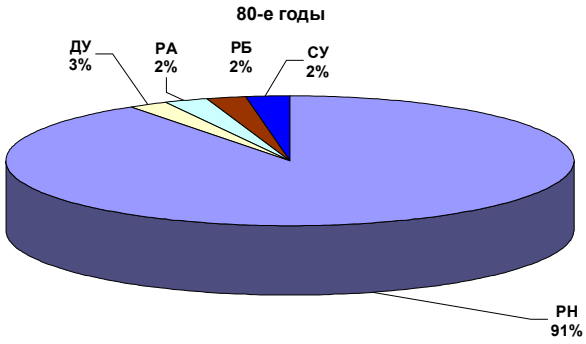


Рис. 9. Распределение причин отказов ракетно-космической техники в 80-е годы

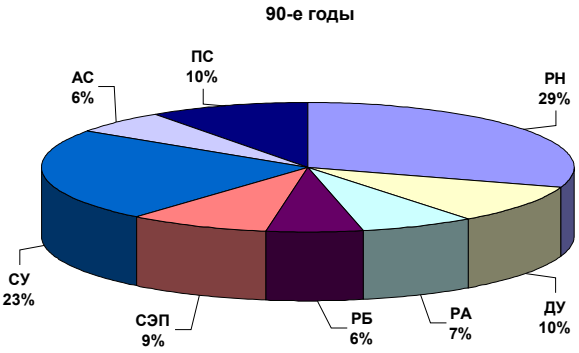


Рис. 10. Распределение причин отказов ракетно-космической техники в 90-е годы

Таблица 5

Риски аварий из-за отказов составляющих РКТ, 90-е годы (в пересчете на один пуск РН)

Причина аварии	Кол-во отказов	Риск аварии
Отказы и взрывы ступеней ракетоносителя (РН)	31	0,036
Отказы двигательных установок (ДУ)	10	0,012
Отказы радиоаппаратуры (РА)	7	0,008
Отказы разгонных блоков (РБ)	6	0,007
Отказы систем электропитания и кабельных сетей (СЭП)	9	0,01
Отказы системы управления (СУ)	24	0,028
Отказы аппаратных средств бортовых компьютеров (АС)	6	0,007
Отказы программных средств бортовых компьютеров (ПС)	10	0,012

Приведенные в табл. 5 значения рисков могут быть уточнены, если учесть дифференциацию рисков для отказов компонент РН и КА.

Проведенный анализ показывает, что наиболее подвержены аварийным отказам ступени РН, второе место занимают системы управления. Однако современный этап характеризуется появлением новых рисков, которые обусловлены применением в бортовых системах управления компьютерной техники. Отказы программных средств (ПС) бортовых компьютеров вместе с отказами двигательных установок делят 3 - 4 место среди всех причин отказов. В среднем из-за отказов ПС заканчивается аварией каждый 100-й пуск (в среднем – раз в год). Следует отметить, что аппаратные средства (АС) отказывают почти в два раза реже, чем ПС. В табл. 6 приведены данные об отказах АС и ПС бортовых компьютеров с 1996 по 2000 гг.

6. Компьютерные средства и системы как фактор риска аварий АРКТ

Учитывая нарастающую динамику влияния надежности компьютерных средств и систем на безопасность АРКТ, проанализируем более детально факторы риска, связанные с этими компонентами. Такой анализ проведем с учетом нарастающей тенденции применения в авиационных и ракетно-космических компьютерных системах (и других критических приложениях) ранее спроектированных аппаратных и программных средств собственной разработки или коммерческих решений [10, 11].

В качестве примера наиболее серьезных отказов по вине ПС можно привести взрыв европейского ракетоносителя Ariane-5 4.06.1996 г. [12]. Анализ этой аварии позволяет сделать ряд общих выводов, относящихся к специфике использования ПС в системах управления АРКТ. Ariane-5 был аварийно подорван через 40 секунд после старта по сигналу бортового компьютера управления. Сигнал был выдан из-за неверной интерпретации нештатной ситуации: переполнение переменной в функции, которая не оказывала влияния на полет ракеты. Убытки от аварии составили более чем полмиллиарда долларов.

Таблица 6

Отказы бортовых компьютеров КА за период с 1996 по 2000 гг.

Дата аварии	Дата пуска	Тип РН	Тип КА	Место отказа (РН/КА)	Причина отказа (АС/ПС)	Страна-изготовитель	Причина отказа
04.06.96	04.06.96	Ariane-5	4 науч. спут. «Cluster F»	РН	ПС	ЕС	Переполнение операнда вызвало выдачу БК ошибочной команды и привело к автоподрыву РН
08.09.97	20.02.86	Протон 8К82К	ОС «Мир»	КА	АС	СССР	На орбитальном комплексе "Мир" отказал бортовой компьютер. Нарушена ориентация комплекса, отключены некоторые бортовые системы
17.08.97	20.02.86	Протон 8К82К	ОС «Мир»	КА	ПС	СССР	Из-за ошибки в программе БК не состоялась повторная стыковка грузового корабля "Прогресс М-35" и орбитального комплекса "Мир"
02.01.98	23.09.97	Космос-3М	FAISAT-2V	КА	АС	США	Неисправности в БК. Эти проблемы привели к снижению мощности солнечных батарей и к неустойчивой работе аппаратуры в тени Земли
04.07.98	18.12.93	Ariane-4.44L	DBS-1	КА	АС	США	На борту КА "DBS-1" произошел отказ управляющего процессора SCP. Управление было автоматически передано на резервный процессор и аппарат продолжил работу без последствий для обслуживаемых им клиентов
20.07.98	18.10.89	МТКК OV-104 «Atlantis №5»	Космический зонд «Galileo»	КА	ПС	США	Было обнаружено аномальное поведение одной из двух подсистем, ответственных за прием команд с Земли. КА перешел в режим защиты от ошибок. 23.07.1998 г. специалистам Лаборатории реактивного движения в Пасадене удалось устранить неисправности, для этого потребовалось послать на зонд корректирующую программу, которая смогла заменить собой дефектные элементы в ПС бортового компьютера
27.11.98	18.10.89	МТКК OV-104 «Atlantis №5»	Космический зонд «Galileo»	КА	ПС	США	Два сбоя в ПС, произошедших с интервалом в 6 часов, привели к потере части информации, которую ученые надеялись собрать о Юпитере и спутниках планеты
30.07.99	20.02.86	Протон 8К82К	ОС «Мир»	КА	ПС	СССР	На орбитальном комплексе "Мир" при проведении очередного эксперимента из-за ошибки в составлении программы вышла из строя вычислительная машина ЦВМ-1. Ориентация комплекса нарушилась, что заставило отказаться от проведения ряда запланированных исследований и экспериментов. Ориентация комплекса была восстановлена через 4 дня после аварии
23.09.99	11.12.98	Delta-2-7425	АМС «Mars Klimate Orbiter»	КА	ПС	США	Навигационная ошибка из-за того, что футы и дюймы не были переведены в метрическую систему. Станция прошла через атмосферу Марса и сгорела
20.12.99	18.12.99	Atlas-2AS	Terra	КА	АС	США	Отказ БК. Специалистам NASA удалось восстановить работу бортового компьютера 02.01.2000 г.
12.03.00	12.03.00	Зенит-3SL	ICO F1	РН	ПС	Украина	Логическая ошибка в программе наземной автоматизированной системы предстартовой подготовки. Не была выдана команда на закрытие клапана пневмосистемы 2-й ступени, что привело к остановке двигателя

Положение и ориентация ракеты-носителя в пространстве измеряются инерциальной навигационной системой (Inertial Reference Systems – IRS), составной частью которой является встроенный компьютер, вычисляющий углы и скорости на основе информации от бортовых гироскопов и акселерометрами. Данные от IRS передаются по специальной шине на бортовой компьютер (БК), который обеспечивает необходимую для реализации программы полета информацию и непосредственно – через гидравлические и сервоприводы – управляет твердотопливными ускорителями и двигателем. Для обеспечения надежности используется дублирование оборудования. Поэтому две системы IRS (одна – основная, другая – ее «горячий» резерв) с идентичным аппаратным и программным обеспечением функционируют параллельно. Как только БК обнаруживает, что основная IRS вышла из штатного режима, он сразу же переключается на другую.

Проанализируем причины, приведшие к возникновению отказов ПС.

Во-первых, как ни парадоксально это звучит, одной из основных причин отказов ПС явился положительный опыт предыдущей эксплуатации.

Предыдущая модификация ракетоносителя (Ariane-4) успешно запускалась более 100 раз, при ее запуске никогда не возникало проблем с ПС. Однако Ariane-5 и Ariane-4 имели различия в эксплуатационных профилях. Эти различия заключались в разных траекториях полета, а также в различной предполетной подготовке. Поэтому работа отказавшего программного модуля после момента старта вообще не имела смысла. Однако модуль повторно использовался без каких-либо модификаций из-за нежелания изменять программный код, который успешно работает.

Во-вторых, причиной отказа ПС явилось изменение условий эксплуатации (изменение эксплуатационного профиля).

Допущенные и так и не выявленные программные ошибки обусловлены некорректной практикой повторного использования ПС. В ПС ракетоносителя была оставлена функция предполетной регулировки инерциальной платформы, выполнение которой не требовалось для Ariane-5 (непредусмотренная функция). Первоначальное требование на продолжение выполнения операции регулировки после взлета ракеты было заложено более чем за 10 лет до рокового события, когда проектировались еще ранние модели серии Ariane. Роковую роль сыграло отсутствие точной спецификации повторно используемого модуля. Расследование показало, что обнаружить требование, устанавливающее максимальную величину операнда, переполнение которого привело к катастрофе, можно было с большим трудом: оно затерялось в приложениях к основной спецификации. Кроме того, в самом коде на этот счет не было никаких комментариев, не говоря уже о ссылке на документ с обоснованием этого требования.

Следует отметить, что при анализе общих (нефункциональных) требований к проекту Ariane-5 не была выявлена взаимная противоречивость между необходимостью обеспечения надежности ПС и ограничением максимально допустимой нагрузки на компьютер. В результате для отказавшего программного модуля было принято потенциально опасное компромиссное решение о защите от переполнения не всех семи, а только четырех переменных. Хотя любой инженерный процесс предполагает принятие компромиссных решений в условиях множества разноречивых требований, информация, на основании которой такие решения принимаются, должна быть максимально полной. Следовательно, без полной и точной спецификации нельзя обеспечить корректное повторное использование программных компонентов.

В-третьих, саморазрушение системы фактически было обусловлено требованиями к обеспечению

безопасности и их неадекватно жесткой реализацией. Анализ механизма обработки исключительных ситуаций выявил достаточно грубую проектную ошибку. При сбое ПС компьютер требовал остановки системы, при этом не применялись процедуры восстановления. Таким образом, требования к безопасности вызвали саморазрушение системы. Реализация именно такого механизма явилась следствием распространенной при разработке критических систем проектной культуры – радикально реагировать на возникновение случайных сбоев. Принцип действий здесь исходит из критериев безусловного обеспечения максимальной надежности: отключать допустившее сбой оборудование и тут же задействовать резервный блок. Вероятность того, что этот блок также выдаст случайный сбой, да еще в той же ситуации, для аппаратных систем чрезвычайна мала.

Однако, такой принцип не учитывает особенностей ПС, дефекты которых одинаковым образом проявляются во всех резервных каналах. В данном случае возник отказ по общей причине, обусловленный систематической программной ошибкой, которая обязательно повторяется при одинаковых входных условиях. Поэтому подключение резервной навигационной системы ничего не дало: ведь ПС на ней были те же. Перечисленные выше причины и их взаимосвязь подчеркивают комплексный анализ проблемы. Поэтому, ***в-четвертых***, в качестве еще одной причины отказов ПС следует указать недостаточный объем процесса его верификации и валидации и компьютерной системы в целом.

Процесс верификации спецификаций, кода и документов с обоснованием проектных решений при разработке ПС для Ariane-5 оказался неадекватен. В частности, к процессу верификации не привлекались специалисты из организаций, независимых как от заказчика, так и от производителя системы, что нарушило принцип разделения исполнительных и контрольных функций. Кроме того, на этапе тестирования и отладки системы было технически возможно в рамках интегрального моделирования процесса полета исследовать все аспекты работы IRS, что позволило бы почти гарантированно выявить ошибку, приведшую к аварии. Однако, вместо этого при моделировании работы всего комплекса IRS рассматривалась как черный ящик, заведомо выдающий то, что ожидается. Анализ отказов ПС системы управления ракетоносителя Ariane-5 показал взаимосвязь явлений, возникающих при повторном использовании ПС и компьютеров для различных аэрокосмических и других критических приложений. Это указывает на объективный характер существующей проблемы и необходимость ее всестороннего анализа при повторном использовании компонент компьютерных систем.

7. Анализ рисков аварий авиационной техники и их сопоставление с РКТ

Проведенный анализ аварий авиационной техники за 80-е годы и начало 90-х годов [10] позволяет установить их причины (см. табл. 7). Основными среди них в порядке убывания частоты являются: ошибочные действия экипажа, отказы авиационной техники, ошибки персонала (наземных служб), непредусмотренные условия эксплуатации. Что касается причин аварий, обусловленных отказами авиационной техники, то по ним обобщенные данные отсутствуют. В табл. 8 символом “+“ (“±“) отмечены те подсистемы, которые содержат (могут содержать) встроенные компьютерные средства, отказы которых могут привести к авариям. Очевидно, что за последние десятилетия развитие авионики и информационных технологий привело к насыщению систем АТ компьютерными средствами, а следовательно, увеличило риски аварий из-за их отказов. Если сравнить риски аварий АТ и РКТ (рис. 11), то можно сделать вывод о превалировании для АТ человеческого фактора, с которым связано 72% аварий, при этом доминируют ошибочные действия экипажа.

В РКТ значение человеческого фактора намного меньше и составляет 2%, что имеет вполне понятное объяснение. Кроме того, среди причин аварий АТ, в отличие от РКТ, имеют место причины, связанные с непредусмотренными условиями эксплуатации, которые являются достаточно весомым фактором аварий.

Таблица 7

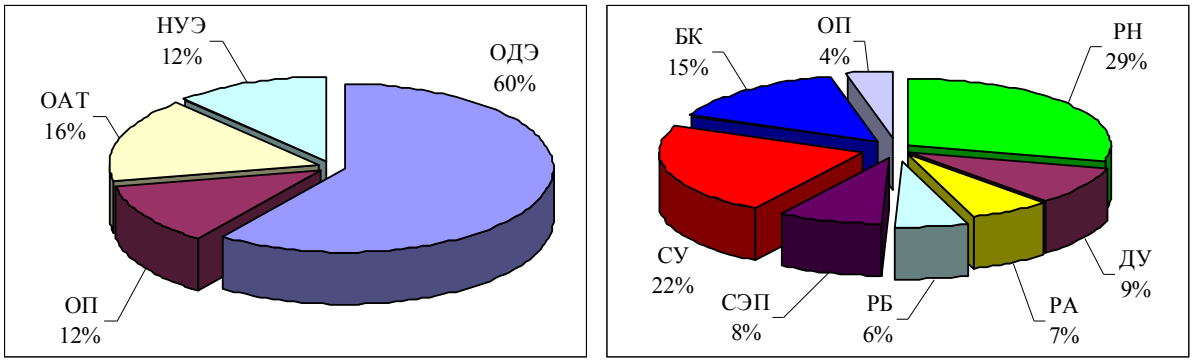
Классификация причин аварий в авиации

Ошибочные действия экипажа (ОДЭ), 60%	Ошибки персонала (ОП), 12%	Отказы авиационной техники (ОАТ), 16%	Попадание самолета в непредусмотренные условия эксплуатации (НУЭ), 12%
Взаимодействие в системе «человек-самолет»	Трудоемкость обслуживания	Несущие агрегаты	Сложные метеорологические условия
		Фюзеляж	
Окружающая среда	Окружающая среда	Посадочные устройства	Климатические и природные условия
Профессиональные факторы	Профессиональные факторы	Силовая установка	Биологические факторы
		Системы управления	
Потеря работоспособности	Потеря работоспособности	Гидросистема	Столкновения с птицами
		Пневмосистема	
Профессиональная подготовка	Профессиональная подготовка	Система жизнеобеспечения экипажа	Столкновения с большими объектами
Халатность	Халатность	Система электроподачи	Повреждения от грузов
		Бортовая радиоаппаратура	Незаконные вмешательства

Таблица 8

Наличие компьютерных систем в оборудовании самолетов

Несущие агрегаты	Фюзеляж	Посадочные устройства	Силовая установка	Системы управления	Гидросистема	Пневмосистема	Система жизнеобеспечения экипажа	Система электроподачи	Бортовая радиоаппаратура
–	–	±	±	+	±	±	+	+	+



а б

Рис. 11. Диаграммы причин аварий АТ (а) и РКТ (б) (80-90-е годы)

Заключение. Направления дальнейших исследований

В статье выполнен анализ рисков АРКТ, который позволил выявить следующие тенденции, присущие современному этапу ее развития:

1) значение рисков для аварий РН колеблется в диапазоне 0,05…0,10;

2) значение рисков для аварий КА во второй половине 90-х годов превзошло аналогичный показатель для РН и составляет 0,15…0,20;

3) аварии РКТ из-за отказов программных средств во второй половине 90-х годов происходили в среднем один раз в год (1 отказ на 100 пусков РН). Следует отметить, что ПС бортовых компьютеров отказывают чаще, чем АС, а для РН отказы аппарат-

ных средств вообще не характерны из-за короткого времени работы;

4) среди аварий АТ, в отличие от РКТ, неизмеримо больший вес имеют риски, связанные с человеческим фактором.

Дальнейшие исследования целесообразно проводить в следующих направлениях:

1) уточнение статистики за счет анализа новых данных об отказах и авариях АТ и РКТ и проведение регрессионно-корреляционнонго анализа статистических данных для прогноза будущих тенденций развития АРКТ;

2) уточнение модели оценки рисков с учетом составляющих РН и КА и последствий аварии;

3) проведение сопоставительного анализа причин аварий, в частности, при внедрении новых информационных и других технологий с иными критическими приложениями [1];

4) разработка методов и средств повышения надежности и безопасности СУ и бортовых компьютеров на основе внедрения отказоустойчивых проектных решений [11];

5) исследование методов снижения влияния дефектов ПС на аварии АРКТ путем создания и использования инструментальных систем поддержки экспертизы и верификации, внедрения многоверсионных технологий.

Литература

1. Айзенберг Е.Я., Ястребенецкий М.А. Сопоставление принципов обеспечения безопасности систем управления ракетами-носителями и атомными электростанциями // Космічна наука і технологія.– 2002.– Т. 8.– № 1.– С. 55 - 60.

2. Лабенский В.Б. Применение корреляционно-регрессионного анализа при планировании работ в ракетно-космической отрасли // Проблемы управления и информатики.– 2001.– № 4.– С. 101 - 110.

3. Радаев Н.Н. Повышение точности прогноза вероятности катастроф за счет ущерба неоднородных статистических данных по ущербу // Автоматика и телемеханика. – 2000. – № 3. – С. 183 - 189.

4. Железняков А.Б. Взлетая, падала ракета…– СПб.: Система, 2003. – 220 с.

5. Харченко В.С., Скляр В.В., Тарасюк О.М. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций // Радіоелектронні і комп'ютерні системи. – Х.: НАКУ «ХАІ». – 2003. – Вип. 3. – С. 135 - 149.

6. Филиппов В. Обеспечение надежности авиационной техники и вооружения в США // Зарубежное военное обозрение. – 1991. – №3. – С. 39 - 46.

7. Фигуровский Д. Повышение надежности авиационного радиоэлектронного оборудования // Зарубежное военное обозрение. – 1988. – № 1. – С. 49-52.

8. Филиппов В. Исследования в США перспективных направлений развития авиационно-космической техники // Зарубежное военное обозрение. – 1990. – № 6. – С. 31 - 38.

9. Риженко О.І., Рябков В.І. Особливі польотні ситуації та причини їх виникнення на літаках і вертольотах: Навчальний посібник. – Х.: Міносвіти України, 1998. – 288 с.

10. Харченко В.С., Скляр В.В., Кожемяченко В.Г. Классификация и профилирование OTS-продуктов для компьютерных систем управления // Системи обробки інформації. – Х.: ХВУ. – 2003. – Вип. 2. – С. 38 - 44.

11. Харченко В.С., Юрченко Ю.Б. Анализ структур бортовых комплексов при использовании электронных компонент Industry // Технология и конструирование в электронной аппаратуре. – 2003. – №2. – С. 3 - 11.

12. Аджиев В. Мифы о безопасном ПО: уроки знаменитых катастроф // Открытые Системы. – 1999. – № 6. – С. 3 - 23.

Поступила в редакцию 7.01.04

Рецензент: д-р техн. наук, профессор Жихарев В.Я., Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.