УДК 004.056.53:629.78 DOI 10.18698/2308-6033-2017-7-1634

Метод оценки стойкости функций безопасности средств защиты автоматизированной системы управления полетами космических аппаратов

© А.Г. Андреев[1], Г.В. Казаков[1], В.В. Корянов[2]

[1]ФГБУ «4 ЦНИИ» Минобороны России,
г. Королёв, Московской обл., 141091, Россия
[2]МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Значительное число факторов риска воздействует на автоматизированную систему управления полетами (АСУП) космических аппаратов. Для их эффективной нейтрализации необходимо оценить показатели чувствительности и стойкости средств защиты информации АСУП. Для различных классов защищенности таких систем необходимо определить базовые функциональные показатели безопасности. При этом исходят из понятия стойкости функций безопасности, для оценки значения которой введены строгие определения базовых понятий: механизма защиты, средства защиты, достоверности контроля, чувствительности и стойкости средств защиты информации. Для коэффициента защищенности, являющегося показателем стойкости средств защиты информации, получено аналитическое выражение. С использованием типовой модели процесса противодействия угрозе решена задача определения некоторых ориентировочных значений вероятностей ошибок 2-го рода для средств защиты. Проведена оценка приоритетов средств защиты информации, что позволило получить вариационный ряд значений вероятностей ошибок 2-го рода, и в определенных случаях задать требуемые значения таких вероятностей средств защиты. Применение разработанного метода дает возможность оценить остаточное воздействие угрозы на информационные ресурсы автоматизированной системы управления полетами космических аппаратов. Если величина остаточного риска является допустимой, то стойкость механизмов защиты отвечает требованиям безопасности системы. В противном случае необходимо использовать механизмы защиты повышенной стойкости.

Ключевые слова: *информационная безопасность, локализация угрозы, механизм защиты, нейтрализация угрозы, обнаружение угрозы, предотвращение возникновения угрозы, средство защиты, стойкость системы управления, чувствительность средства защиты*

Введение. Под стойкостью автоматизированной системы управления полетами космических аппаратов (АСУП КА) понимается свойство системы выполнять свои функции и сохранять свои параметры в пределах установленных значений во время и после воздействия на нее факторов риска [1] в течение всего срока службы в заданных условиях эксплуатации.

Цель оценки стойкости функций безопасности — выявление степени устойчивости АСУП КА, выступающей объектом оценки, по отношению к атакам нарушителя с определенно низким, умеренным или высоким потенциалом нападения [2–6].

В ГОСТ Р ИСО/МЭК 15408-3–2013 отмечается, что количественную оценку стойкости функций безопасности можно получить только для механизма защиты (МЗ), реализованного в виде парольной защиты. В работе [7] представлены методики оценки уровня информационной безопасности (ИБ), в которых реализованы требования к надежному криптографическому программному обеспечению. В работе [8] исследовано влияние параметров алгоритма многоитерационного хеширования с несколькими модификаторами на его криптостойкость. Оценка стойкости функций безопасности рассмотрена в ГОСТ Р 52633.3–2011 с позиций тестирования программных средств аутентификации как показатель, определяющий число попыток подбора, необходимое злоумышленнику для получения на выходе преобразователя неизвестного ему кода доступа «Свой» при использовании для атаки заранее сформированной базы биометрических образов «Чужой».

Применение в информационных системах интеллектуальных карт в качестве «шифровальной машинки» с аппаратно реализованным алгоритмом блочного шифрования и хранящимися на ней ключами шифрования рассмотрено в работе [9]. Критерии построения алгоритмов отрицаемого шифрования для реализации механизмов защиты информации типа обманных ловушек изложены в работе [10].

В работах [11–13] предложены варианты оценки стойкости функций безопасности технических средств защиты. Применение математического аппарата теории массового обслуживания и «теории катастроф» рассмотрено с точки зрения злоумышленного изучения технического средства в действии [11]. В работе [13] дана оценка возможности применения распределенных информационных систем при оценке стойкости радиоэлектронной аппаратуры к воздействию заряженных частиц космического пространства.

В то же время оценка стойкости функций безопасности за систему в целом в настоящее время носит общий характер. К примеру, в статье [14] предложена методика оценки защищенности информационной системы. Ее суть сводится к тому, что для каждого актива, в том числе и для средств защиты информации, необходимо определить достаточный уровень стойкости функций безопасности, проверить их на соответствие требованиям стандартов и, наконец, сделать вывод о состоянии его защищенности.

Однако можно получить выражение, позволяющее вычислить количественное значение оценки показателя стойкости функций безопасности для любых видов механизмов защиты информации с помощью модели процесса противодействия угрозе.

Методические основы оценки стойкости функций безопасности средств защиты АСУП КА. Различным классам защищенности АСУП соответствуют базовые функциональные показатели безопас-

ности, которые можно определить исходя из понятия стойкости функций безопасности. Последняя, в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013, является «характеристикой функции безопасности объекта оценки, выражающей минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности».

Очевидно, что такое определение стойкости функции безопасности не является конструктивным и не позволяет даже на интуитивном уровне в качественных величинах оценить ее значение, например, в шкале «высокий — средний — низкий», поскольку содержит такие неопределенные термины, как «интуитивный уровень», «предположительно», «ожидаемого». В связи с этим введем более строгие определения некоторых базовых понятий.

Определение 1. Механизм защиты (МЗ) — это метод, методика или способ, направленные на реализацию установленного непустого множества функций безопасности.

Полное множество функций безопасности для средства защиты информации включает: предотвращение (п), обнаружение (о), локализацию (л), нейтрализацию (н) угрозы и восстановление (в) безопасного состояния АСУП КА.

Определение 2. Средство защиты (СЗ) — это реализация физическими, техническими, программными средствами, организационными мерами заданного механизма защиты для выполнения определенных функций безопасности.

Реализация функции безопасности, связанной с обнаружением угрозы в любом средстве защиты информации, всегда основана на выделении хотя бы одного контролируемого параметра, сравнение текущего и требуемого значений которого позволяет реализовать эту функцию безопасности. Из сказанного следует, что средства защиты информации в любом исполнении, с формальной точки зрения, являются средствами контроля. Для этих средств выделяют три основные характеристики: достоверность контроля, чувствительность и стойкость.

Определение 3. Достоверность контроля — свойство средства защиты обнаруживать и противостоять попытке угрозы $У_j$ нарушить установленные характеристики безопасности защищаемых активов АСУП КА.

Любой механизм защиты, реализованный в виде изделия информационной технологии с функцией защиты информации от воздействия угрозы, имеет всего четыре состояния с вероятностями:

1) $P_{ПП}$ — вероятность восприятия правильной информации как правильной;

2) P_{α} — вероятность ошибки первого рода;

3) $P_{\text{НН}}$ — вероятность восприятия неправильной информации как неправильной;

4) P_{β} — вероятность ошибки второго рода.

В первом и третьем состояниях средство защиты информации от воздействия угрозы $У_j$ функционирует правильно, а во втором и четвертом — имеет место ошибочное реагирование механизма защиты на входной сигнал:

- угрозы нет, но средство защиты информации «считает», что она присутствует;
- угроза есть, но средство защиты информации «считает», что ее нет.

Из определения достоверности контроля следует, что ее показатель $D_{\text{КНТ}}$ определяется вероятностями принятия правильных решений, т. е. выражением вида

$$D_{\text{КНТ}} = P_{\text{ПП}} + P_{\text{НН}}. \quad (1)$$

Поскольку перечисленные четыре состояния средства защиты информации составляют полную группу, вероятность того, что оно находится в одном из этих состояний:

$$P_{\text{ПП}} + P_{\text{НН}} + P_{\alpha} + P_{\beta} = 1. \quad (2)$$

Из выражений (1) и (2) получим более удобное для практического использования выражение вида

$$D_{\text{КНТ}} = 1 - (P_{\alpha} + P_{\beta}).$$

Ошибка второго рода наиболее опасна, поскольку приводит к реализации угрозы вторжения в информационные ресурсы АСУП КА, воздействие которой способно нанести существенный (неприемлемый) ущерб целям выполнения задачи КА вследствие нарушения конфиденциальности, целостности или доступности информационных ресурсов АСУП КА.

Ошибка первого рода приводит к появлению непредвиденных временных затрат на выяснение причины «ложной тревоги», поскольку входная информация не содержит признаков реализации угрозы (вторжения) и необходимо дополнительное время, чтобы провести анализ и убедиться в этом. Ошибка первого рода нарушает только одну характеристику ИБ защищаемых активов АСУП КА — их доступность.

К АСУП КА предъявляются высокие требования по оперативности процесса подготовки данных полета КА, поэтому опасность ошибок как второго, так и первого родов соизмерима.

Из определения достоверности контроля следует, что эта характеристика средств защиты может быть представлена двумя свойствами: чувствительностью и стойкостью.

Определение 4. Чувствительность средства защиты — способность средства защиты обнаруживать наличие реально существующей угрозы, для защиты от которой оно предназначено.

Определение 5. Стойкость средства защиты — способность средства защиты противостоять попытке угрозы проникнуть к информационным активам АСУП КА, в том числе и путем его обхода (подмены) или «взлома».

Определение 6. Показателем чувствительности средства защиты информации $Ч_{СЗ}$ служит величина, зависящая от вероятности ошибки второго рода:

$$Ч_{СЗ} = 1 - P_{\beta}.$$

Определение 7. Показателем стойкости функций безопасности средства защиты информации $С_{СЗ}$ является коэффициент защищенности $К(зщ)_j$:

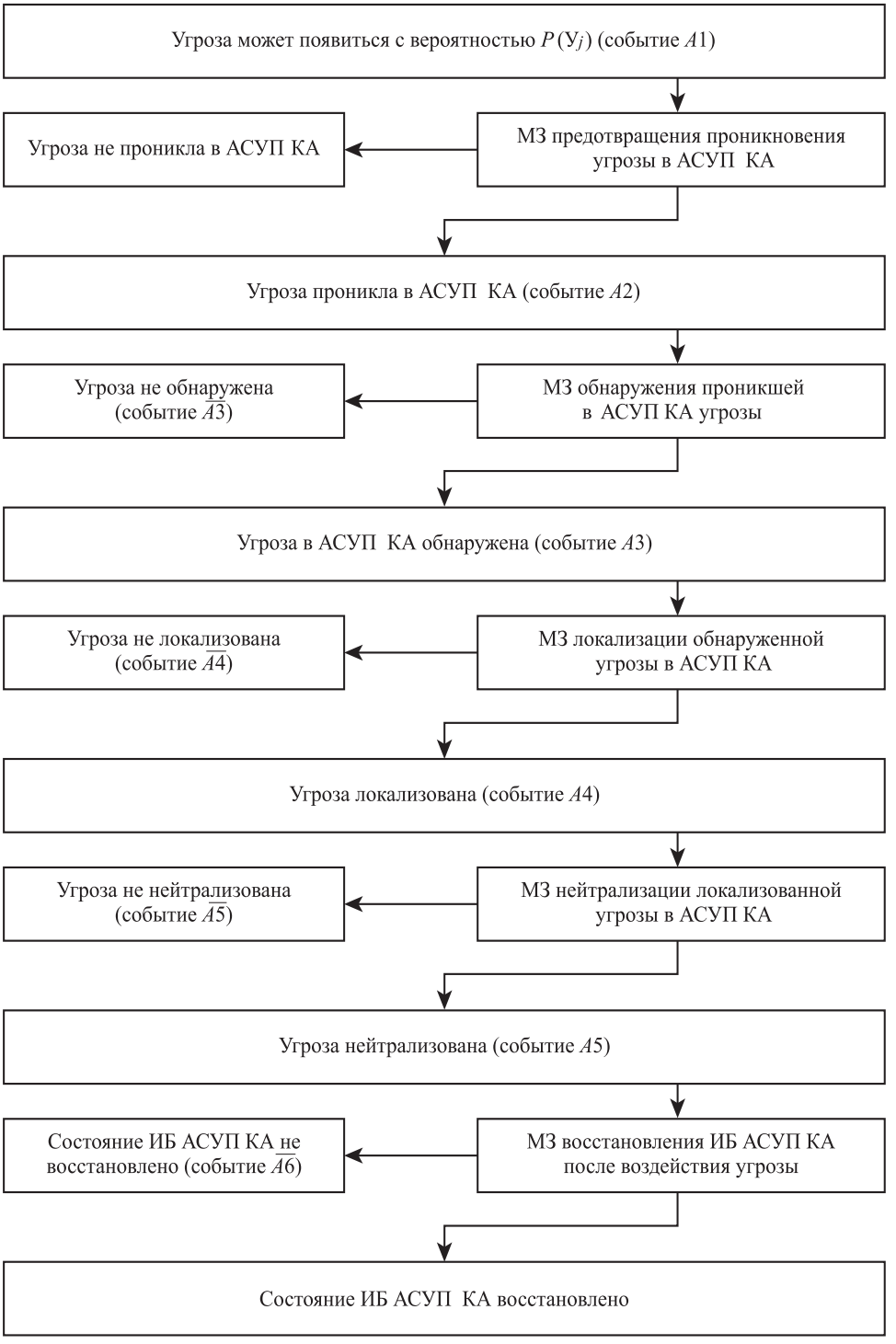
$$С_{СЗ} = К(зщ)_j = 1 - К(ов)_j, \qquad (3)$$

где $К(ов)_j$ — коэффициент остаточного воздействия угрозы $У_j$ после преодоления ею всех функций безопасности средств защиты.

Коэффициент остаточного воздействия угрозы $У_j$ на информационные ресурсы АСУП КА можно определить, исходя из типовой модели процесса противодействия угрозе, показанной на рисунке в виде орграфа $Г$. Характеристики модели противодействия угрозе — величины вероятностей ошибок второго рода для каждого из видов средств защиты информации.

При анализе величин вероятностей ошибок второго рода средств защиты информации, необходимо учитывать три основных фактора: 1) политику безопасности, реализуемую каждым из видов средств защиты; 2) конкретную реализацию средств защиты в виде физических, программно-аппаратных средств и организационно-технических мер, выполняющих определенные функции безопасности по защите информационных ресурсов АСУП КА от воздействия угроз; 3) адекватность средства защиты информации с точки зрения соответствия его стоимости и значимости предъявляемым к нему требованиям по обеспечению безопасности защищаемых информационных ресурсов АСУП КА (под стоимостью СЗ понимается не столько стоимость разработки (приобретения), сколько время его функционирования в структуре АСУП КА).

При использовании модели процесса противодействия угрозе необходимо иметь исходные данные, используемые в алгоритмах анализа рисков АСУП КА.



Орграф Г модели процесса противодействия угрозе

Перечислим вероятности ошибки второго рода для каждого из видов функций безопасности, выполняемых средствами защиты информации:

- $P_{\beta}(\text{п})_j$ — для предотвращения проникновения угрозы У_j в АСУП КА;
- $P_{\beta}(\text{о})_j$ — для обнаружения проникшей в АСУП КА угрозы;
- $P_{\beta}(\text{л})_j$ — для локализации угрозы в информационных ресурсах (ИР) АСУП КА;
- $P_{\beta}(\text{н})_j$ — для нейтрализации угрозы;
- $P_{\beta}(\text{в})_j$ — для восстановления ИБ АСУП КА.

Введем еще одну характеристику — вероятность $P(\text{У}_j)$ появления угрозы У_j. Ее значение примем равным либо 1 при расчете потенциального риска нанесения ущерба целям применения АСУП КА угрозой У_j, либо величине коэффициента КПР(У_j) (коэффициента потенциальной реализуемости угрозы У_j, равной потенциалу реализации угрозы ее источником) при расчете остаточного риска нанесения ущерба целям применения АСУП КА.

С использованием модели процесса противодействия угрозе можно получить как общие алгоритмы оценки остаточного риска, так и характеристики МЗ.

Метод оценки коэффициента защищенности АСУП КА. В соответствии с моделью процесса противодействия угрозе определяются события Ai и противоположные им $\overline{Ai}$, от которых зависит появление главного события A_j, заключающегося в наличии остаточного воздействия угрозы на ИР АСУП КА (после преодоления угрозой У_j всех функций безопасности средств защиты информации). Вероятность этого события обозначим через $P(A_j)$. Главное событие A_j зависит от некоторых составных событий B_k, которые определяются в соответствии с табл. 1.

В табл. 1 символом + обозначен факт причастности событий Ai или $\overline{Ai}$ к появлению главного события A_j, связанного с потенциальным наличием остаточного воздействия угрозы на ИР АСУП КА.

Если в ячейке табл. 1 стоит символ +, то вероятность соответствующего события Ai или $\overline{Ai}$ равна $P(Ai)$ или $P\left(\overline{Ai}\right)$, а если стоит 1, то это и есть вероятность наступления события Ai.

Таблица 1

Состав событий, приводящих к появлению события A_j

Событие	**Угроза** $У_i$								ИБ не восстановлена
	появилась	проникла в систему	обнаружена	не обнаружена	локализована	не локализована	нейтрализована	не нейтрализована	
$Ai\,/\overline{Ai}$	$A1$	$A2$	$A3$	$\overline{A3}$	$A4$	$\overline{A4}$	$A5$	$\overline{A5}$	$\overline{A6}$
Вероятности появления событий $\boldsymbol{Ai\,/\overline{Ai}}$									
$P(Ai)\,/\,P(\overline{Ai})$	$P(У_j)$	$P_β$(п)	$1-P_β$(о)	$P_β$(о)	$1-P_β$(л)	$P_β$(л)	$1-P_β$(н)	$P_β$(н)	$P_β$(в)
Вероятности появления событий B_k									
B_1	+	+	+	–	–	+	–	+	+
B_2	+	+	–	+	–	**1**	–	**1**	**1**
B_3	+	+	+	–	+	–	–	+	+
B_4	+	+	+	–	+	–	+	–	+

Вероятности определенной совокупности событий A_i определяют потенциальную вероятность $P(A_j)$ появления главного события A_j.

Составим различные комбинации событий Ai и $\overline{Ai}$, исходя из условия появления главного события A_j, в соответствии с обозначениями табл. 1. В результате получим четыре составных события B_k, которые приводят к появлению главного события A_j с вероятностью $P(A_j)$:

$$B_1 = A1 \cap A2 \cap A3 \cap \overline{A4} \cap \overline{A5} \cap \overline{A6},$$
$$B_2 = A1 \cap A2 \cap \overline{A3} \cap \overline{A4} \cap \overline{A5} \cap \overline{A6},$$
$$B_3 = A1 \cap A2 \cap A3 \cap A4 \cap \overline{A5} \cap \overline{A6},$$
$$B_4 = A1 \cap A2 \cap A3 \cap A4 \cap A5 \cap \overline{A6}.$$

Определим вероятности появления событий B_k. Обозначим через $P(B_k)$ вероятности появления события B_k. Тогда в соответствии с табл. 1 эти вероятности будут равны:

$$P(B_1) = P(У_j)P_β(п)_j(1-P_β(о)_j)P_β(л)_j P_β(н)_j P_β(в)_j,$$
$$P(B_2) = P(У_j)P_β(п)_j P_β(о)_j,$$
$$P(B_3) = P(У_j)P_β(п)_j(1-P_β(о)_j)(1-P_β(л)_j)P_β(н)_j P_β(в)_j,$$
$$P(B_4) = P(У_j)P_β(п)_j(1-P_β(о)_j)(1-P_β(л)_j)(1-P_β(н)_j)P_β(в)_j.$$

Задача — получить выражение для оценки потенциальной вероятности появления главного события A_j.

Из приведенных представлений событий B_k в виде пересечения событий Ai и $\overline{Ai}$, видно, что они несовместны, поскольку каждое из событий B_k содержит хотя бы одно из противоположных событий Ai или $\overline{Ai}$, которые, по определению, являются несовместными ($Ai \cap \overline{Ai} = \varnothing$, где $\varnothing$ — символ пустого множества). Следовательно, вероятность появления главного события A_j будет равна:

$$P(A_j) = P(B_1) + P(B_2) + P(B_3) + P(B_4). \quad (4)$$

Далее определим вероятности появления событий Ai и $\overline{Ai}$:

- $A1$ (появление угрозы для АСУП КА)

$$P(A1) = P(\text{У}_j); \quad (5)$$

- $A2$ (угроза проникла в АСУП КА вследствие наличия ошибки второго рода МЗ предупреждения проникновения в нее угрозы)

$$P(A2) = P_{\beta}(\text{п})_j; \quad (6)$$

- $\overline{A3}$ (угроза в АСУП КА не обнаружена из-за наличия ошибки второго рода средства защиты)

$$P(\overline{A3}) = P_{\beta}(\text{о})_j; \quad (7)$$

- $A3$ (угроза обнаружена в АСУП КА, но сам факт обнаружения угрозы еще не означает, что она исключает наличие события A_j)

$$P(A3) = 1 - P_{\beta}(\text{о})_j; \quad (8)$$

- $A4$ (угроза локализована, но сам факт локализации угрозы также не означает, что она не приведет к событию A_j)

$$P(A4) = 1 - P_{\beta}(\text{л})_j; \quad (9)$$

- $\overline{A4}$ (угроза не локализована из-за наличия ошибки второго рода МЗ локализации угрозы в АСУП КА)

$$P(\overline{A4}) = P_{\beta}(\text{л})_j; \quad (10)$$

- $A5$ (угроза нейтрализована)

$$P(A5) = 1 - P_{\beta}(\text{н})_j; \quad (11)$$

• событие $\overline{A5}$ (угроза не нейтрализована из-за наличия ошибки второго рода СЗ, нейтрализующего угрозу, но факт нейтрализации угрозы не обеспечивает отсутствия события A_j)

$$P(\overline{A5}) = P_{\beta}(\text{н})_j; \tag{12}$$

• событие $\overline{A6}$ (безопасное состояние АСУП КА не восстановлено из-за наличия ошибки второго рода СЗ по восстановлению ее ИБ)

$$P(\overline{A6}) = P_{\beta}(\text{в})_j. \tag{13}$$

Определим вероятность появления главного события A_j.

После подстановки выражений (5)–(13) в формулу (4) и алгебраических преобразований полученной суммы будет получено выражение для определения вероятности наступления главного события:

$$\begin{aligned} P(A_j) = P(\text{У}_j)P_{\beta}(\text{п})_j \left\{ P_{\beta}(\text{в})_j (1 - P_{\beta}(\text{о})_j) \times \right. \\ \left. \times \left[P_{\beta}(\text{н})_j + (1 - P_{\beta}(\text{л})_j)(1 - P_{\beta}(\text{н})_j) \right] + P_{\beta}(\text{о})_j \right\}. \end{aligned} \tag{14}$$

Из выражения (14) следует, что вероятность $P(A_j)$ определяется произведением вероятности появления угрозы $P(\text{У}_j)$ на некоторый коэффициент К_j, зависящий от характеристик средств защиты АСУП КА, которые «ослабляют» (нейтрализуют) воздействие угрозы.

Запишем общепринятое выражение для потенциального риска $R_{\text{П}}$, который может отрицательно сказаться на выполнении целей применения любой автоматизированной системы:

$$R_{\text{П}} = P(\text{У}_j)\text{УЩ}_j, \tag{15}$$

где УЩ_j — величина ущерба, наносимого целям применения АСУП КА при воздействии угрозы У_j.

Величину остаточного риска $R_{\text{о}}$ воздействия угрозы можно вычислить по формуле

$$R_{\text{о}} = P(\text{У}_j)\text{К(ов)}_j\,\text{УЩ}_j, \tag{16}$$

где К(ов)_j — коэффициент, отражающий степень остаточного воздействия угрозы У_j на информационные ресурсы АСУП КА.

Физический смысл выражения (16) определяется следующим образом: если защита идеальная, т. е. $\text{К(ов)}_j = 0$, то $R_{\text{о}} = 0$, что и сле-

дует из формулы (16), а если защита отсутствует, т. е. $К(ов)_j = 1$, то $R_о = R_П$, что следует из выражений (15) и (16).

Главное событие A_j не определяет риск нанесения ущерба целям применения АСУП КА, следовательно, вероятность главного события в соответствии с выражением (16) может быть записана в виде

$$P(A_j) = P(У_j)К(ов)_j,$$

где, как следует из выражения (14),

$$К(ов)_j = P_β(п)_j \left\{ P_β(п)_j (1 - P_β(о)_j) \times \right.$$
$$\left. \times \left[P_β(н)_j + (1 - P_β(л)_j)(1 - P_β(н)_j) \right] + P_β(о)_j \right\}. \quad (17)$$

Можно показать, что полученное формальным путем аналитическое выражение для $К(ов)_j$ обладает семантической правильностью, т. е. в количественном эквиваленте отражает смысл защиты АСУП КА при использовании соответствующих видов МЗ. Для этого необходимо определить значение $К(ов)_j$ при двух «идеальных критичных» условиях:

1) все СЗ идеально выполняют свои функции (вероятности их ошибок второго рода равны 0);

2) все СЗ не выполняют свои функции (вероятности их ошибок второго рода равны 1).

Пусть в соответствии с первым условием $P_β(q)_j = 0$ (где $q =$ п, о, л, н, в). Тогда $К(ов)_j$ должен быть равен 0, что означает «абсолютное» ослабление угрозы, поскольку СЗ работают «идеально».

Из выражения (17) имеем:

$$К(ов)_j = 0\left\{0(1-0)\left[0 + (1-0)(1-0)\right] + 0\right\} = 0.$$

Из уравнения (3) следует, что

$$К(зщ) = 1 - К(ов) = 1.$$

Пусть в соответствии со вторым условием $P_β(q)_j = 1$ (где $q =$ п, о, л, н, в). Тогда коэффициент остаточного воздействия угрозы $К(ов)_j$ должен быть равен 1, что означает отсутствие МЗ, т. е. АСУП КА является не защищенной, в связи с чем угроза беспрепятственно наносит ущерб информации (раскрывает, искажает, подменяет, блокирует и уничтожает информационные ресурсы АСУП КА).

Из выражений (3) и (17) следует

$$К(ов)_j = 1\{1(1-1)[1+(1-1)(1-1)]+1\} = 1\{1\cdot 0[1+0]+1\} = 1.$$

Таким образом, показано, что аналитическое выражение (17) соответствует физическому смыслу защиты информационных ресурсов АСУП КА от воздействия угрозы $У_j$.

Очевидно, что при $P(У_j)=1$ значение $P_р(A_j)$ численно равно коэффициенту $К(ов)_j$. Вероятность «реального» наличия остаточного воздействия угрозы $У_j$ на информационные ресурсы АСУП КА $P_р(A_j)$ может быть получена, если вероятность появления угрозы принять равной не единице, а потенциалу источника реализации угрозы (злоумышленным или случайным) $ПРУ(У_j)$. Тогда

$$P_р(A_j) = ПРУ(У_j)К(ов)_j.$$

Заметим, что в зависимости от вида угрозы и способа реализации конкретной АСУП КА не все фазы процесса противодействия угрозе могут иметь место в явном виде, поэтому число событий Ai может быть другим (в данном случае оно уменьшится). В этом случае в выражении для $К(ов)_j$ не следует учитывать вероятности ошибок второго рода функций тех средств защиты, которые не используются для защиты АСУП КА. Например, если против угрозы раскрытия конфиденциальной информации АСУП КА применены достаточно эффективные средства защиты, предотвращающие проникновение к ней несанкционированных лиц, то модель процесса противодействия этой угрозе будет содержать лишь один этап — предотвращение проникновения угрозы к конфиденциальной информации АСУП КА. В этом случае, как следует из формулы (17), выражение примет вид

$$К(ов)_j = P_β(п)_j.$$

Для оценки остаточных (потенциального и реального) рисков защищенной АСУП КА необходимо задать требуемое значение коэффициента защищенности $К_j^Т(зщ)$.

В зависимости от значения коэффициента $К_j^Т(зщ)$ необходимо определить допустимые значения вероятностей ошибок второго рода используемых средств защиты в конкретной АСУП КА. Поскольку, как следует из выражения (17), допустимые значения вероятностей ошибок второго рода средств защиты АСУП КА связаны функциональной зависимостью с допустимым значением коэффициента остаточного воздействия угрозы $К_j^Т(ов)$, эти вероятности нельзя задать произвольно.

В связи с этим возникает задача определения допустимых значений вероятностей ошибок второго рода используемых средств защиты АСУП КА в зависимости от допустимого значения $К_j^{Д}(ов)$, которое, в свою очередь, линейно зависит от требуемого значения коэффициента защищенности АСУП КА:

$$К_j^{Т}(зщ) = 1 - К_j^{Д}(ов).$$

Эта задача имеет значительную степень неопределенности, что не позволяет получить точное решение. По этой причине для ее решения предлагается метод, связанный с предварительной оценкой некоторых «опорных» значений этих вероятностей.

Метод определения «опорных» значений характеристик средств защиты. Для получения требуемых значений величин вероятностей ошибок второго рода используемых средств защиты АСУП КА, с формальной точки зрения, необходимо решить уравнение

$$\begin{aligned} К_j^{Д}(ов) = P_{\beta}^{Д}(п)_j \Big\{ P_{\beta}^{Д}(в)_j (1 - P_{\beta}^{Д}(о)_j) \times \\ \times \Big[P_{\beta}^{Д}(н)_j + (1 - P_{\beta}^{Д}(л)_j)(1 - P_{\beta}^{Д}(н)_j) \Big] + P_{\beta}^{Д}(о)_j \Big\}, \end{aligned} \tag{18}$$

где допустимые значения вероятностей ошибок второго рода видов СЗ $P_{\beta}^{Д}(п)_j$, $P_{\beta}^{Д}(о)_j$, $P_{\beta}^{Д}(л)_j$, $P_{\beta}^{Д}(н)_j$, $P_{\beta}^{Д}(в)_j$ неизвестны, а допустимое значение $К_j^{Д}(ов)$ является заданной величиной. Следовательно, имеем одно уравнение с пятью неизвестными.

Для определения допустимых значений указанных вероятностей ошибок второго рода есть два пути: во-первых, получить недостающее число линейно независимых уравнений, составляющих базис в линейном пространстве, и получить хорошо обусловленную матрицу взаимосвязи неизвестных, определитель которой значительно отличался бы от нуля; во-вторых, задать все неизвестные величины, кроме одной, которую и надлежит определить.

Получить необходимое число линейно независимых уравнений не представляется возможным, значит, остается второй путь получения допустимых значений вероятностей ошибок второго рода для пяти видов функций безопасности СЗ.

Используя модель процесса противодействия угрозе, можно поставить задачу определения некоторых ориентировочных значений вероятностей ошибок второго рода для перечисленных видов СЗ, которые назовем «опорными» значениями. Для их определения необходимо оценить приоритеты (коэффициенты чувствительности к степени защищенности АСУП КА) перечисленных видов СЗ, которые соответ-

ствуют этапам модели процесса противодействия угрозе. Для этого предлагается способ, заключающийся в выполнении двух действий:

- учета степени чувствительности величины $К_j^{Д}(ов)$ к различным видам функций безопасности СЗ;
- получения наиболее информативных сведений о взаимной важности видов функций МЗ относительно друг друга, что обеспечивается использованием матрицы парных сравнений этих функций.

Для оценки чувствительности $К_j^{Д}(ов)$, необходимо составить варианты исходных данных таким образом, чтобы по ним можно было оценить чувствительность величины $К_j^{Д}(ов)$, равную ее приращению $\Delta К_j^{Д}(ов)$ при вариациях вероятностей ошибок второго рода последовательно для каждого из видов функций безопасности средств защиты. Очевидно, что эти исходные данные должны содержать пять вариантов (по числу видов указанных выше функций безопасности СЗ).

Каждый вариант должен содержать одинаковые значения вероятностей ошибок второго рода для всех видов СЗ, равные, например, 0,4, за исключением одного, который определяет вариант исходных данных. Для этого вида функций безопасности СЗ определяется вариация вероятности ошибки второго рода, находящаяся, например, в пределах 0,1–0,2. Для всех пяти вариантов используются данные табл. 2.

Таблица 2

Варианты исходных данных для расчета остаточного риска АСУП КА

Наименование исходных данных	Варианты исходных данных				
	1	2	3	4	5
$P(У_j)$	**1,0**	**1,0**	**1,0**	**1,0**	**1,0**
$P_β(п)_j$	**0,1–0,2**	0,4	0,4	0,4	0,4
$P_β(о)_j$	0,4	**0,1–0,2**	0,4	0,4	0,4
$P_β(л)_j$	0,4	0,4	**0,1–0,2**	0,4	0,4
$P_β(н)_j$	0,4	0,4	0,4	**0,1–0,2**	0,4
$P_β(в)_j$	0,4	0,4	0,4	0,4	**0,1–0,2**

Используя приведенные данные (см. табл. 2), дважды вычисляем вероятность $К_j^{Д}(ов)$ по формуле (17) : 1) для вероятности ошибки второго рода выбранного вида функции безопасности СЗ, равной 0,1; 2) для этой же вероятности, равной 0,2, при значениях вероятностей ошибок второго рода остальных видов функций СЗ, равных 0,4.

В результате определяем приращения $\Delta К_j^{Д}(ов)$ при варьировании значений вероятности ошибки второго рода одного из видов функций МЗ при неизменных значениях вероятности ошибок второго рода для остальных видов функций безопасности СЗ.

Результаты вычислений приращений $\Delta К_j^{Д}(ов)$ с использованием формулы (17), их ранжирование по возрастанию (важности) и соответствие видов СЗ величинам $\Delta К_j^{Д}(ов)$ представлены в табл. 3.

Таблица 3

Результаты расчетов $\Delta К_j^{Д}(ов)$ и ранжирование функций безопасности СЗ по возрастанию

Виды функций безопасности СЗ	**Значения $\Delta К_j^{Д}(ов)$**	**Ранжированные по важности виды СЗ**	**Вариационный ряд для $\Delta К_j^{Д}(ов)$**
Предотвращение	0,021	Предотвращение	**0,060**
Обнаружение	0,112	Обнаружение	**0,030**
Локализация	0,046	Восстановление	**0,010**
Нейтрализация	0,064	Локализация	**0,004**
Восстановление	0,021	Нейтрализация	**0,016**

Из данных табл. 3 видно, что величина $К_j^{Д}(ов)$ наиболее чувствительна к функции безопасности СЗ:

- по предотвращению проникновения угрозы в АСУП КА;
- по обнаружению проникшей угрозы в АСУП КА.

Для этих видов СЗ приращение $\Delta К_j^{Д}(ов)$ имеет наибольшие значения. К остальным видам функций МЗ величина $К_j^{Д}(ов)$ менее чувствительна, что отражено в последнем столбце табл. 3.

Можно показать, что полученные числовые значения отвечают физическому смыслу процесса защиты АСУП КА. С формальной точки зрения, коэффициент $К(ов)_j$ должен удовлетворять только одному условию: защищенность АСУП КА должна быть не ниже требуемой, т. е.

$$К(ов)_j \le К_j^{Д}(ов).$$

Однако это требование не учитывает важность каждого из видов СЗ в процессе защиты ИР АСУП КА. К примеру, можно определить функции безопасности СЗ таким образом, чтобы доминировала функция СЗ по восстановлению ИБ АСУП КА. Но это не отвечает физическому смыслу ее защиты от воздействия угрозы, поскольку такая политика функции безопасности приведет к тому, что АСУП

КА будет подвержена воздействию угрозы с нанесением целям ее функционирования неприемлемого ущерба, только потом ИБ АСУП КА будет восстанавливаться.

Очевидно, что физический смысл процесса защиты АСУП КА заключается в том, чтобы, во-первых, предотвратить проникновение угрозы к активам АСУП КА, во-вторых, обнаружить проникшую в АСУП КА угрозу. Затем локализовать ее, нейтрализовать и восстанавливать состояние ее ИБ в случае, если СЗ не выполнит своих функций по предотвращению и выявлению угрозы из-за наличия методической или инструментальной ошибки второго рода.

Исходя из физического смысла процесса защиты, можно сформулировать политику функции безопасности таким образом, чтобы функция СЗ по предотвращению проникновения угрозы к ИР АСУП КА и функция МЗ по обнаружению проникшей в ИР АСУП КА угрозы были бы равнозначными и имели наивысший приоритет по сравнению с другими видами функций МЗ.

Используя данные табл. 3, составим матрицу парных сравнений $\mathbf{M}(\text{сз})$ видов функций безопасности СЗ по признаку сравнения «величина вероятности ошибки второго рода». При этом необходимо учесть условие: чем чувствительнее величина $К_j^{Д}(\text{ов})$ к вероятности ошибки второго рода какого-либо вида функции безопасности СЗ, тем меньше должна быть величина вероятности ошибки второго рода для этого вида функции безопасности. Полученная в результате сравнения матрица приведена в табл. 4. В ней использованы следующие обозначения функций безопасности СЗ: Н — по нейтрализации угрозы; Л — по локализации угрозы; В — по восстановлению ИБ АСУП КА; О — по обнаружению угрозы; П — по предупреждению проникновения угрозы в АСУП КА, а также $W(\text{сз})_q$ — вектор приоритетов видов СЗ.

Таблица 4

Матрица парных сравнений М(сз) для видов функций безопасности средств защиты информации АСУП КА

Обозначение функций	Н	Л	В	О	**П**
Н	**1,00**	2,00	4,00	7,00	9,00
Л	0,50	**1,00**	2,00	4,00	5,00
В	0,25	0,50	**1,00**	2,00	2,00
О	0,14	0,25	0,50	**1,00**	1,00
П	0,11	0,20	0,50	1,00	**1,00**
$W(\text{сз})_q$	**0,50**	**0,27**	**0,12**	**0,06**	**0,05**

Отношение согласованности этой матрицы равно $OS = 0,001$.

Поскольку при составлении матрицы **М**(сз) в качестве признака сравнения была использована вероятность ошибки второго рода каждого из видов СЗ, собственный вектор этой матрицы определяет некоторые значения вероятностей ошибок второго рода всех видов МЗ, которые назовем «опорными» значениями.

Таким образом, «опорные» значения вероятностей ошибок второго рода (отмечены символом *), полученные с помощью матрицы парных сравнений этих вероятностей для всех видов функций безопасности СЗ, с учетом чувствительности величины $К_j^{Д}(ов)$ удовлетворяют следующей цепочке неравенств

$$P_{β}^{*}(п)_j \le P_{β}^{*}(о)_j < P_{β}^{*}(в)_j < P_{β}^{*}(л)_j < P_{β}^{*}(н)_j. \qquad (19)$$

С качественной стороны, эта цепочка неравенств отражает взаимозависимость величин ошибок второго рода разных видов функций безопасности СЗ, ее необходимо соблюдать при определении их требуемых значений. Подставив «опорные» значения вероятностей ошибок второго рода видов СЗ в выражение для $К_j^{Д}(ов)$, получим «опорное» значение коэффициента остаточного воздействия угрозы

$$К_j^{*}(ов) = 0,05\left\{0,12(0,94)\left[1-0,27(0,5)\right]+0,06\right\} = 0,007.$$

Таким образом, если заданное значение коэффициента $К_j^{Д}(ов) = 0,007$ ($К_j^{Т}(зщ) = 1 - К_j^{Д}(ов) = 0,993$), то в качестве требуемых значений вероятностей ошибок второго рода видов функций безопасности СЗ можно принять их опорные значения. Если требуемое значение $К_j^{Т}(зщ) = 0,999$, то требуемые значения вероятностей ошибок второго рода видов функций безопасности СЗ подбираются таким образом, чтобы удовлетворялась цепочка неравенств (19).

Для этого случая в качестве требуемых значений вероятности ошибки второго рода функции МЗ по предотвращению проникновения угрозы к информационным ресурсам АСУП КА примем величину $P_{β}^{Д}(п)_j = 0,01$. Исходя из условия (18), примем $P_{β}^{Д}(о)_j = 0,01$. Тогда

$$К_j^{Д}(ов) = 0,01\left\{0,12(0,94)\left[1-0,135\right]+0,01\right\} = 0,001.$$

В результате $К_j^{Т}(зщ) = 0,999$, что и требовалось обеспечить.

Заключение. Одни из основных задач обеспечения информационной устойчивости АСУП КА в части обеспечения ее ИБ — разработка не только моделей угроз и защиты, но и модели противодей-

ствия угрозе, которая позволяет количественно оценить стойкость функций безопасности используемых средств защиты информации. В связи с этим был разработан метод оценки показателя стойкости функции безопасности любого СЗ, основанный на общей модели процесса противодействия угрозы. При его разработке были получены следующие результаты: определены такие базовые понятия, как механизм и средство защиты, достоверность контроля, осуществляемого средствами защиты, и ее показатель, чувствительность и стойкость механизмов защиты и их показатели. Введение перечисленных понятий позволило разработать в общем виде модель противодействия угрозе с помощью специфических событий Ai и противоположных им $\overline{Ai}$. Использование таких событий и вероятностей их появления позволило получить аналитическое выражение для вероятности $P(A_j)$ наступления главного события A_j, заключающегося в наличии остаточного воздействия угрозы на информационные ресурсы АСУП КА.

ЛИТЕРАТУРА

[1] Андреев А.Г, Казаков Г.В., Корянов В.В. Метод определения факторов риска для автоматизированной системы управления полетами космических аппаратов. *Инженерный журнал: наука и инновации*, 2016, вып. 7. URL: http://dx.doi.org/10.18698/2308-6033-2016-7-1511

[2] Бородакий Ю.В., Добродеев А.Ю., Нащекин П.А., Бутусов И.В. О подходах к реализации централизованной системы управления информационной безопасностью АСУ военного и специального назначения. *Вопросы кибербезопасности*, 2014, № 2 (3), с. 2–9.

[3] Марков А.С., Цирлов В.Л., Барабанов А.В. *Методы оценки несоответствия средств защиты информации.* Москва, Радио и связь, 2012, 192 с.

[4] Цирлов В.Л. *Основы информационной безопасности. Краткий курс.* Ростов-на-Дону, Феникс, 2008, 254 с.

[5] Полянский Д.А. *Оценка защищенности.* Владимир, Изд-во Владим. гос. ун-та, 2005, 80 с.

[6] *Руководящий документ. Безопасность информационных технологий. Положение по обеспечению безопасности в жизненном цикле изделий информационных технологий.* Москва, ФСТЭК России, 2004, 54 с.

[7] Авдошин С.М., Савельева А.А. Криптографические методы защиты информационных систем. *Известия АИН им. А.М. Прохорова. Бизнес-информатика*, 2006, т. 17, с. 91–99.

[8] Вихман В.В., Панков М.А. Повышение стойкости хеш-функций в информационных системах на основе алгоритма многоитерационного хеширования с несколькими модификаторами. *Труды СПИИРАН*, 2014, вып. 5 (36), с. 194–205.

[9] Варфоломеев А.А. *Защита информации с использованием интеллектуальных карт.* Москва, РУДН, 2008, 87 с.

[10] Морозова Е.В., Мондикова Я.А., Молдовян Н.А. Способы отрицаемого шифрования с разделяемым ключом. *Информационно-управляющие системы*, 2013, № 6 (67), с. 73–78.

[11] Васильев К.К., Глушков В.А., Дормидонтов А.В., Нестеренко А.Г. *Теория электрической связи.* Ульяновск, УлГТУ, 2008, 452 с.

[12] Косолапов Ю.В. *Способ защиты информации от технической утечки, основанный на применении кодового зашумления и кодовых криптосистем. Дис. … канд. техн. наук.* Ростов-на-Дону, 2009, 169 с.

[13] Пашковская Е.С., Пашковский М.Е., Барабанов В.Ф. Разработка программной среды распределенной системы оценки стойкости полупроводниковых изделий. *Вестник Воронежского государственного технического университета*, 2013, № 4, с. 4–7.

[14] Бондарь И.В., Золотарев В.В., Попов А.М. Методика оценки защищенности информационной системы по требованиям стандартов информационной безопасности. *Моделирование систем*, 2010, № 4, с. 3–12.

Статья поступила в редакцию 29.03.2017

Ссылку на эту статью просим оформлять следующим образом:

Андреев А.Г., Казаков Г.В., Корянов В.В. Метод оценки стойкости функций безопасности средств защиты автоматизированной системы управления полетами космических аппаратов. *Инженерный журнал: наука и инновации*, 2017, вып. 7. http://dx.doi.org/10.18698/2308-6033-2017-7-1634

Статья подготовлена по материалам доклада, представленного на XLI Академических чтениях по космонавтике, посвященных памяти академика С.П. Королёва и других выдающихся отечественных ученых — пионеров освоения космического пространства. Москва, МГТУ им. Н.Э. Баумана, 24–27 января 2017 г.

Андреев Анатолий Георгиевич — канд. техн. наук, старший научный сотрудник ФГБУ «4 ЦНИИ» Минобороны России. Автор более 70 работ в области надежности автоматизированных систем управления. e-mail: kgv.64@mail.ru

Казаков Геннадий Викторович — канд. техн. наук, доцент, начальник управления ФГБУ «4 ЦНИИ» Минобороны России. Автор более 70 работ в области надежности автоматизированных систем управления. e-mail: kgv.64@mail.ru

Корянов Всеволод Владимирович — канд. техн. наук, доцент, первый заместитель заведующего кафедрой «Динамика и управление полетом ракет и космических аппаратов» МГТУ им. Н.Э. Баумана. Автор более 40 публикаций.
e-mail: vkoryanov@bmstu.ru

Method for assessing safety functions durability of the security facility of an automated spacecraft flight control system

© A.G. Andreev[1], G.V. Kazakov[1], V.V. Koryanov[2]

[1]Federal State Budget Institution the 4th Central Research Institute
of the Ministry of Defence of the Russian Federation,
Korolev town, Moscow Region, 141091, Russia
[2]Bauman Moscow State Technical University, Moscow, 105005, Russia

A significant number of risk factors affect the automated spacecraft flight control system (ASFCS). To effectively neutralize these factors, it is necessary to assess the sensitivity and stability of the information security facility of the ASFCS. For different security classes of such systems, it is necessary to define basic functional safety indicators. We rely on the notion of security functions durability, and for its evaluation we introduce strict definitions of the basic concepts: the mechanism of protection, security facility, reliability of control, sensitivity and durability of information security facility. For the security coefficient, which is an indicator of the durability of information security facility, we obtained an analytical expression. Using the standard model of the threat counteraction process, we solved the task of determining some tentative values of type 2 error probabilities for the security facility. Furthermore, we assessed the priorities of the information security facility, which enabled us to obtain a variational series of type 2 error probability values, and in certain cases to set the required values of such probabilities of the security facility. The application of the developed method makes it possible to assess the residual threat impact on the information resources of the automated spacecraft flight control system. If the residual risk is acceptable, then the stability of the protection mechanisms meets the requirements of the system's safety. Otherwise, it is necessary to use protection mechanisms with the increased durability.

***Keywords**: information security, threat localization, protection mechanism, threat neutralization, threat detection, threat prevention, security facility, durability of control system, sensitivity of security facility*

REFERENCES

[1] Andreev A.G., Kazakov G.V., Koryanov V.V. *Inzhenernyy zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation*, 2016, no. 7. Available at: http://dx.doi.org/10.18698/2308-6033-2016-7-1511

[2] Borodakiy Yu.V., Dobrodeev A.Yu., Naschekin P.A., Butusov I.V. *Voprosy kiberbezopasnosti — Cybersecurity issues*, 2014, no. 2 (3), pp. 2–9.

[3] Markov A.S., Tsirlov V.L., Barabanov A.V. *Metody otsenki nesootvetstviya sredstv zaschity informatsii* [Methods for assessing the inconsistency of information secutiry facility]. Moscow, Radio i svyaz Publ., 2012, 192 p.

[4] Tsirlov V.L. *Osnovy informatsionnoy bezopasnosti. Kratkiy kurs* [Fundamentals of Information Security. A Short Course]. Rostov-na-Donu, Feniks Publ., 2008, 254 p.

[5] Polyanskiy D.A. *Otsenka zaschischennosti* [Security assessment]. Vladimir, Vladimir State University Publ., 2005, 80 p.

[6] *Rukovodyaschiy dokument. Bezopasnost informatsionnykh tekhnologiy. Polozhenie po obespecheniyu bezopasnosti v zhiznennom tsikle izdeliy*

in-formatsionnykh tekhnologiy [Guidance document. Security of information technology. The provision for ensuring safety in the life cycle of products of information technology]. Moscow, Federal Service for Technical and Export Control of Russia, 2004, 54 p.

[7] Avdoshin S.M., Saveleva A.A. *Izvestiya AIN im. A.M. Prokhorova. Biznes-informatika — News Academy of Engineering Sciences A.M. Prokhorov*, 2006, vol. 17, pp. 91–99.

[8] *Vikhman V.V., Pankov M.A. Trudy SPIIRAN — SPIIRAS Proceedings, 2014, no. 5 (36), pp. 194–205.*

[9] Varfolomeev A.A. *Zaschita informatsii s ispolzovaniem intellektualnykh kart* [Protection of information using smart cards]. Moscow, RUDN Publ., 2008, 87 p.

[10] Morozova E.V., Mondikova Ya.A., Moldovyan N.A. *Informatsionno-upravlyayushchie sistemy — Information and Control Systems*, 2013, no. 6 (67), pp. 73–78.

[11] Vasilev K.K., Glushkov V.A., Dormidontov A.V., Nesterenko A.G. *Teoriya elektricheskoy svyazi* [The theory of electrical communication]. Ulyanovsk, UlSTU Publ., 2008, 452 p.

[12] Kosolapov Yu.V. *Sposob zashchity informatsii ot tekhnicheskoy utechki, os-novannyi na primenenii kodovogo zashumleniya i kodovykh kriptosistem. Diss. kand. tekhn. nauk* [The method of protecting information from technical leakage, based on the use of code noise and code cryptosystems. Cand. eng. sc. diss.]. Rostov-na-Donu, 2009, 169 p.

[13] Pashkovskaya E.S., Pashkovskiy M.E., Barabanov V.F. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta — The Bulletin of Voronezh State Technical University*, 2013, no. 4, pp. 4–7.

[14] Bondar I.V., Zolotarev V.V., Popov A.M. *Modelirovanie sistem* [System modeling], 2010, no. 4, pp. 3–12.

Andreev A.G., Cand. Sc. (Eng.), Senior Research Scientist, Federal State Budget Institution the 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Author of over 70 research works in the field of automated control system reliability. e-mail: kgv.64@mail.ru

Kazakov G.V., Cand. Sc. (Eng.), Assoc. Professor, Head of Federal State Budget Institution the 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Author of over 70 research works in the field of automated control system reliability. e-mail: kgv.64@mail.ru

Koryanov V.V., Cand. Sc. (Eng.), Assoc. Professor, First Deputy Head of the Department of Dynamics and Flight Control of Rockets and Spacecraft, Bauman Moscow State Technical University. Author of over 40 publications in the field of ballistics simulation and dynamics of space and descent vehicles motion. e-mail: vkoryanov@bmstu.ru