УДК 623.61

Структурно-параметрический метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта

Липатников В. А., Парфиров В. А.

Постановка задачи: *опыт вооруженных конфликтов свидетельствует о существенном увеличении возможностей технической разведки по вскрытию информационно-телекоммуникационной сети (ИТКС) специального назначения (СН), что значительно повышает актуальность проблемы повышения их защищенности. Известные способы управления признаковым пространством ИТКС в интересах повышения защищенности обладают рядом ограничений, что не позволяет их в полной мере использовать для управления элементами ИТКС в условиях динамики развития конфликта. Динамическое управление структурными и функциональными параметрами элементов ИТКС целесообразно осуществлять на основе прогноза изменения частных показателей защищенности в процессе конфликта, при этом, временные и вероятностные показатели оцениваются с учетом изменений составляющих, оказывающих влияние на них. При управлении элементами ИТКС СН приоритет отдается управлению внутренними параметрами с учетом доступности ресурсов на каждом элементе.* ***Целью работы*** *является повышение защиты ИТКС СН в условиях информационного конфликта путем оперативного управления структурными и функциональными параметрами элементов.* ***Задача работы*** *заключается в разработке метода динамического управления параметрами элементов ИТКС СН с учетом изменения их разведывательной защищенности в условиях динамики изменяющейся обстановки.* ***Используемые методы:*** *решение задачи основано на совместном применении методов теории конфликта, теории системного анализа, теории множеств, теории управления, теории оптимизации, теории моделирования и комбинаторики.* ***Новизна:*** *предлагаемый метод является развитии теории методов управления ИТКС СН, элементы новизны представленного решения заключаются в использовании дополнительных исходных данных, учета данных прогнозирования динамики их изменения в процессе развития конфликта, что повышает точность оценки временных и вероятностных параметров защищенности при формировании модели изменений показателей защищенности элементов ИТКС СН, а также учете влияния применения выбранных действий при принятии решений по изменению структурных и функциональных параметров элементов в ходе информационного противоборства.* ***Результат:*** *использование предложенного метода позволяет повысить оперативность и обоснованность реагирования на изменение обстановки при управлении защищенностью ИТКС за счет контроля и прогнозирования текущих значений временных и вероятностных показателей, а также процесса выработки научно обоснованных решений по управлению структурными и функциональными параметрами элементов ИТКС СН. По результатам проведенного моделирования метода подтверждена его адекватность и расширенная функциональность.* ***Практическая значимость:*** *представленные прикладные результаты могут быть реализованы в виде специального программного обеспечения информационно-аналитических комплексов в системах поддержки принятия решений по защите ИТКС. Кроме этого, предложенный метод может найти применение при создании интеллектуальных систем управления нового поколения не только ИТКС, но и при проактивном управлении другими техническими системами, функционирующими в условиях информационного конфликта.*

Библиографическая ссылка на статью:
Липатников В. А., Парфиров В. А. Структурно-параметрический метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта // Системы управления, связи и безопасности. 2023. № 4. С. 105-156. DOI: 10.24412/2410-9916-2023-4-105-156

Reference for citation:
Lipatnikov V. A., Parfirov V. A. Structural-parametric method of protection of information and telecommunication network of special purpose in the conditions of information conflict. *Systems of Control, Communication and Security*, 2023, no. 4, pp. 105-156 (in Russian). DOI: 10.24412/2410-9916-2023-4-105-156

Ключевые слова: *информационно-телекоммуникационная сеть, защищенность, управление, конфликт, алгоритм, динамика изменения, система мониторинга и разведки, управление ресурсами.*

Актуальность

Опыт вооруженных конфликтов свидетельствует о том, что возможность взаимного воздействия противоборствующими сторонами на объекты, особенно мобильные, во многом определяется актуальностью и достоверностью данных технической разведки [1-4]. Отсюда следует, что при защите объектов специального назначения вопросы обеспечения разведывательной защищенности (РЗ) выходят на одно из главных мест.

Информационно-телекоммуникационные сети (ИТКС) специального назначения (СН) противоборствующих сторон во время ведения конфликта с одной стороны являются источником разведывательных сведений, заключенных в режимах работы средств и комплексов связи, изменении топологии ИТКС, циркулирующей в ней информации и т.д. С другой стороны, как техническая основа системы управления ИТКС СН является объектом первоочередного поражения, приводящего к дезорганизации управляемых объектов. Таким образом, в независимости от сценариев использования полученных данных об ИТКС противоборствующей стороной требуется обеспечить необходимые значения показателей РЗ ее элементов [5-8].

Современные возможности сторон конфликта по ведению разведки и поражению с высокой вероятностью скоплений техники, расположенной на ограниченной территории [1, 3, 4], вынуждают проводить трансформацию подходов в организации и применению ИТКС СН. От традиционных узлов связи, содержащих в своем составе большое количество аппаратных связи, переходят к более компактным и высокомобильным средствам связи [4, 9, 10]. В переходный период совместно с традиционными узлами связи могут использоваться ретрансляторы, расположенные на БПЛА, средства связи двойного и гражданского назначения и т.д. Называть новые составляющие ИТКС СН узлами связи в полной мере в соответствии с общепринятой терминологией [11] является не совсем корректным, однако, исследовать их РЗ является объективной необходимостью. Поэтому, в данной статье принят общий термин, характеризующий составляющие ИТКС СН, – элемент ИТКС. Под элементом ИТКС в статье понимается узел связи в традиционной форме, группа средств связи или одиночное средство связи, действующее обособленно.

Информационно-телекоммуникационные сети СН являются сложными объектами, которые могут располагаться на значительных территориях, из-за этого их отдельные элементы обладают различным уровнем доступности для системы разведки противоположной стороны конфликта. Поэтому, управлять ими требуется, осуществляя воздействие на элементы ИТКС СН.

Вопросы управления РЗ элементов ИТКС решались в работах [12-22].

В работе [12] предложена модель конфликта, которая на основе методов теории игр позволяет учесть различные комбинации структур ИТКС и вариантов дестабилизирующих воздействий. Показано, что применение дестабилизи-

рующих воздействий основано на данных, получаемых системой разведки конфликтующих сторон. За рамками данной работы остались методы управления РЗ объектов конфликтующих сторон в интересах обеспечения заданных требований.

Работы [13-19], направленные на разработку способов повышения РЗ путем реализации различных технических мероприятий по управлению параметрами средств и комплексов связи и воздействию на средства разведки. Однако, в данных работах не исследуются вопросы управления параметрами ИТКС в привязке к динамике развития конфликта и учета наличия ресурсов по управлению элементами ИТКС СН.

В работах [20, 21] предложены различные алгоритмы управления демаскирующими признаками элементов ИТКС в интересах повышения РЗ, эффективности маскировки и устойчивости. Однако, в предложенных алгоритмах не в полной мере осуществлен учет возможных изменений оперативной обстановки в условиях ведения конфликта. В частности, при управлении демаскирующими признаками не учтены возможные изменения в: структуре и возможностях системы разведки противника; планируемых оперативных задачах, возникающих во время применения ИТКС СН по назначению; качества функционирования ИТКС СН; доступности ресурсов для реализации различных действий по защите элементов ИТКС СН от разведки.

Работа [22] посвящена исследованию технологических основ построения автоматических высокодинамичных систем связи. Определены условия выполнения процесса управления системой связи, содержание оперативно-тактической информации и ее использование при управлении. Обоснованы условия обеспечения эффективного функционирования системы связи группировки в современных специальных действиях. Определены требования к организации и осуществлению сбора, обработки, хранения и передачи оперативно-тактической информации, требования к принимаемым решениям по связи для обеспечения эффективного функционирования системы связи. Однако, в указанной работе отсутствуют алгоритмы, описывающие процесс динамического управления устойчивым функционированием ИТКС СН в условиях динамики течения и развития конфликта.

Таким образом, задача управления ИТКС СН путем управления параметрами ее элементов, влияющими на показатели РЗ, в целях их поддержания в требуемых пределах в процессе конфликта является актуальной.

Целью данной статьи является повышение эффективности процесса управления ИТКС СН в динамике развития конфликта.

Постановка задачи

Задачей статьи является разработка метода защиты ИТКС СН в условиях информационного конфликта.

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

Таблица 1 – Обозначения

Обозначение	Физический смысл обозначения
$P_{РЗдоп.i}$	– минимальное допустимое значение вероятности разведывательной защищенности (вероятностный критерий разведывательной защищенности)
$N_{ИТКС}$	– количество элементов, входящих в состав ИТКС СН
i	– номер элемента ИТКС СН, i=1, ..., $N_{ИТКС}$
M_i	– количество параметров, характеризующих i-й элемент ИТКС СН
O_i	– множество параметров, характеризующих i-й элемент ИТКС СН, $O_i = \{o_{i,m_i}\}$, m_i=1, …, M_i
$R=\{r\}$	– множество параметров, характеризующих систему разведки нападающей стороны
$S=\{s\}$	– множество параметров, характеризующих окружающую среду (физико-географические, климатические условия, уровень помех)
F	– множество параметров, характеризующих ИТКС СН, $F = \bigcup_{i=1}^{N_{ИТКС}} O_i$
F_i	– множество параметров, характеризующих признаковый фон, на котором ведется разведка i-го элемента ИТКС СН (элементы ИТКС СН, в том числе и имитируемые (ложные элементы ИТКС СН), окружающие i-й элемент ИТКС СН, находящиеся в зоне доступности системе разведки нападающей стороны), $F_i = F \setminus O_i$
J_i	– количество типов ресурсов по управлению РЗ i-го элемента ИТКС
$Z_i=\{z_{i,j}\}$	– множество, характеризующих наличие ресурсов по управлению РЗ i-го объекта разведки (элемента ИТКС СН), j=1, …, J_i
G_i	– количество типов параметров, характеризующих качество функционирования i-го элемента ИТКС СН (объекта разведки)
$Q_i = \{q_{i,g_i}\}$	– множество текущих значений параметров, характеризующих качество функционирования i-го элемента ИТКС СН, g_i=1, …, G_i
$Q_{доп.i} = \{q_{доп.i,g_i}\}$	– множество заданных (допустимых) значений параметров, характеризующих качество функционирования i-го элемента ИТКС СН
K_i	– максимально возможное количество действий по повышению РЗ i-го элемента ИТКС СН
k_i =1,..,K_i	– номер действия по повышению РЗ i-го элемента ИТКС СН
$W_i = \{w_{k_i} : \{z_{i,n_{k_i}}\}\}$	– множество действий по повышению РЗ i-го элемента ИТКС СН, каждый элемент которого определяется требующимся для его выполнения множеством ресурсов $\{z_{i,n_{k_i}}\} \in Z_i$, $n_{k_i} \in [1, J_i]$
n_{k_i}	– номер ресурса, который необходим для выполнения k_i-го действия по повышению РЗ i-го элемента ИТКС СН
$tw_{реализ.k_i}$	– время реализации k_i -го действия w_{k_i} из множества W_i по повышению РЗ i-го элемента ИТКС СН
$cw_{реализ.k_i}$	– материальные затраты на реализацию k_i -го действия w_{k_i} из множества W_i по повышению РЗ i-го элемента ИТКС СН
$t_{зад.i}$	– предельное время, в течение которого требуется обеспечить выполнение $P_{РЗдоп.i}$ в заданном районе (временной критерий разведывательной защищенности)
$P_{РЗ\ i}(t)$	– зависимость вероятности РЗ i-го элемента ИТКС СН от времени
$t_{функц.}$	– время функционирования ИТКС СН
t	– время
$Pr_{действ.i}$	– множество признаков реализации наборов действий по повышению РЗ,

Обозначение	Физический смысл обозначения
	$Pr_{\text{действ}i} = \bigcup_{h_i=1}^{K_i} Pr_{\text{действ}i.h_i}$
h_i	– количество действий по повышению РЗ i-го элемента ИТКС СН из множества W_i, h_i=1, …, K_i
$Pr_{\text{действ}i.h_i}$	– множество признаков реализации действий по повышению РЗ i-го элемента ИТКС СН, отражающее возможность применения h_i действий из множества W_i по повышению РЗ для выполнения требований по РЗ
$pr_{\text{действ}i.1\,v_1}$	– v_1-й элемент множества $Pr_{\text{действ}.i.1}$, v_1 =1, …, K_i
$pr_{\text{действ}i.2\,v_1,v_2}$	– v_1, v_2-й элемент множества $Pr_{\text{действ}.\,i.2}$, v_2 =1, ..., K_i
…	…
$pr_{\text{действ}.i.h_i\ v_1,v_2,...,v_{h_i}}$	– v_1, v_2, …, v_{h_i} -й элемент множества $Pr_{\text{действ}i.h_i}$, v_{h_i} = 1, ..., K_i
$T_{\text{реализ}.i}$	– множество, содержащее времена реализации наборов действий по повышению РЗ i-го элемента ИТКС СН, $T_{\text{реализ}.i} = \bigcup_{h_i=1}^{K_i} T_{\text{реализ}.i.h_i}$
$T_{\text{реализ}.i.h_i}$	– множество времен реализации наборов действий по повышению РЗ i-го элемента ИТКС СН, отражающее возможность применения h_i действий из множества W_i, для выполнения требований по РЗ
$t_{\text{реализ}.1\ v_1}$	– время реализации действия по повышению РЗ i-го элемента ИТКС СН, содержащего одно действие с номером v_1 (элемент множества $T_{\text{реализ}.i.1}$)
$t_{\text{реализ}.2\ v_1,v_2}$	– время реализации набора действий по повышению РЗ i-го элемента ИТКС СН, содержащего два действие с номерами v_1 и v_2 (элемент множества $T_{\text{реализ}.i.2}$)
…	…
$t_{\text{реализ}.h_i\ v_1,v_2,...,v_{h_i}}$	– время реализации набора действий по повышению РЗ i-го элемента ИТКС СН, содержащего h_i действий с номерами v_1, v_2, …, v_{h_i} (элемент множества $T_{\text{реализ}.i.h_i}$)
$C_{\text{реализ}.i}$	– множество, содержащее стоимость реализации наборов действий по повышению РЗ i-го элемента ИТКС СН, $C_{\text{реализ}.i} = \bigcup_{h_i=1}^{K_i} C_{\text{реализ}.i.h_i}$
$C_{\text{реализ}.i.h_i}$	– множество стоимостей реализации наборов действий по повышению РЗ i-го элемента ИТКС СН, отражающее возможность применения h_i действий из множества W_i, для выполнения требований по РЗ требований по РЗ
$c_{\text{реализ}.i.1\ v_1}$	– материальные затраты (стоимость) реализации v_1-го действия из множества W_i по повышению РЗ i-го элемента ИТКС СН (элемент множества $C_{\text{реализ}.i.1}$)
$c_{\text{реализ}.i.2\ v_1,v_2}$	– материальные затраты (стоимость) реализации v_1, v_2-го набора действий из множества W_i по повышению РЗ i-го элемента ИТКС СН (элемент множества $C_{\text{реализ}.i.2}$)
…	…
$c_{\text{реализ}.i.h_i\ v_1,v_2,...,v_{h_i}}$	– материальные затраты (стоимость) реализации v_1, v_2, …, v_{h_i} -го набора действий из множества W_i по повышению РЗ i-го элемента ИТКС СН (элемент множества $C_{\text{реализ}.i.h_i}$)
$Pr_{ИТКС}$	– признак изменения информации о состоянии ИТКС СН

Обозначение	Физический смысл обозначения
Pr_{CP}	– признак изменения информации о состоянии системы разведки нападающей стороны
n	– номер набора действий по повышению РЗ, n=0, …, $\left\|Pr_{\text{действ}i}\right\|$

На вербальном уровне задачу работы можно представить [23], как разработку метода M защиты ИТКС СН в условиях конфликта, путем обеспечения выполнения требований по РЗ $P_{\text{РЗ}.i}(t) \geq P_{\text{РЗдоп}.i}$ на заданном интервале времени $t_{\text{зад}.i}$ для каждого элемента ИТКС СН (для $\forall i, i = 1,..., N_{ИТКС}$), на основе:

– прогноза изменения показателей РЗ ИТКС СН $P_{\text{РЗ}.i}(t)$ в течение времени нахождения элемента в заданном районе $t_{\text{зад}.i}$, полученного с учетом вариативности условий обстановки функционирования элементов ИТКС СН, учитывающей изменения внутренних параметров элемента ИТКС СН: режимов функционирования составляющих элемента ИТКС СН O_i; наличия ресурсов по повышению РЗ элемента ИТКС СН Z_i; множества доступных действий по повышению РЗ элемента ИТКС СН W_i; а также изменения внешних параметров, оказывающих влияние на РЗ элемента ИТКС СН: признакового фона F_i, на котором ведется разведка элемента ИТКС СН; окружающей среды S; параметров функционирования системы разведки R;
– определения, из множества допустимых действий W_i, в каждом элементе ИТКС СН доступного, с учетом имеющихся ресурсов Z_i, наборов действий по повышению РЗ $Pr_{\text{действ}.i}$;
– определения и применения оптимального, с учетом минимизации временных $\min\{T_{\text{реализ}.i}\}$, и/или материальных $\min\{C_{\text{реализ}.i}\}$ затрат на реализацию, набора действий по повышению РЗ из множества $Pr_{\text{действ}.i}$, при выполнении заданных требований к качеству функционирования элементов ИТКС СН $Q_{\text{доп}.i}$.

На формальном уровне постановка задачи исследования имеет следующий вид.

Дано: множество F, определяющее состав и параметры элементов ИТКС СН, состоящей из $N_{\text{ИТКС}}$ элементов; множество O_i, определяющее i-й элемент ИТКС СН, i=1, ..., $N_{\text{ИТКС}}$; множество параметров R, характеризующих систему разведки; множество параметров S, характеризующих состояние окружающей среды; множество F_i, определяющее состав и параметры признакового фона, на котором ведется разведка i-го элемента ИТКС СН; множество Z_i, характеризующее наличие ресурсов по управлению РЗ i-го элемента ИТКС СН; множество Q_i, характеризующее качество функционирования i-го элемента ИТКС СН; минимально допустимое значение вероятности разведывательной защищенности (вероятностный критерий разведывательной защищенности) элемента ИТКС СН $P_{\text{РЗдоп}.i}$; множество допустимых значений $Q_{\text{доп}.i}$, характеризующих качество функционирования ИТКС СН; предельное время $t_{\text{зад}.i}$, в течение которого требуется обеспечить выполнение $P_{\text{РЗдоп}.i}$ в заданном районе (временной критерий разведывательной защищенности); множество доступных действий по повышению РЗ W_i; время функционирования ИТКС СН $t_{\text{функц}.}$; время реализации дей-

ствий по повышению РЗ $tw_{\text{реализ.}k_i}$; затраты на реализацию действий по повышению РЗ $cw_{\text{реализ.}k_i}$; множество признаков реализации наборов действий по повышению РЗ $Pr_{\text{действ.}i}$.

Для $\forall i, i = 1,...,N_{ИТКС}$ требуется разработать метод управления параметрами элемента ИТКС СН с учетом доступных ресурсов, направленный на обеспечение требуемого значения показателя РЗ в условиях изменяющейся обстановки, при соблюдении требований к качеству функционирования элемента ИТКС СН по назначению:

$$M :< O_i, R, F_i, S, Z_i, W_i, Q_{\text{доп.}i}, t > \rightarrow P_{\text{РЗ}i}(t) \mid \begin{vmatrix} P_{\text{РЗ}i}(t \le t_{\text{зад.}i}) \ge P_{\text{РЗдоп.}i}, t_{\text{зад.}i} \le t_{\text{функц.}} \\ q_{i,g_i} \ge q_{\text{доп.}i,g_i}, q_{i,g_i} \in Q_i, q_{\text{доп.}i,g_i} \in Q_{\text{доп.}i}, g_i = 1,...,G_i \\ opt\{T_{\text{реализ.}i}, C_{\text{реализ.}i}\} \rightarrow opt\{Pr_{\text{действ.}i}\}, \\ t_{\text{реализ.}i} \in T_{\text{реализ.}i}, t_{\text{реализ.}i} = f(pr_{\text{действ.}i}, tw_{\text{реализ.}i}), \\ c_{\text{реализ.}i} \in C_{\text{реализ.}i}, c_{\text{реализ.}i} = \varphi(pr_{\text{действ.}i}, cw_{\text{реализ.}i}) \end{vmatrix}, \quad (1)$$

где: f, φ – символы функционального преобразования; M – символ искомого преобразования.

Обоснование теоретического базиса решения задачи

Для решения задачи статьи, формально заданной выражением (1), требуется определить аппарат, позволяющий вырабатывать управленческие решения по поддержанию требуемого уровня показателей РЗ элементов ИТКС СН, на основе определения оптимальных наборов параметров элементов ИТКС СН, заданных множеством O_i, с учетом применения доступных действий по повышению РЗ из множества W_i и в соответствии с имеющимися ресурсами Z_i, для условий ведения разведки системой разведки, характеризуемой множеством R, на признаковом фоне, характеризуемом множеством F_i, и с учетом влияния окружающей среды S.

Процесс динамического управления является циклическим процессом, в рамках которого постоянно должны реализовываться этапы подготовки, принятия, реализации и контроля выполнения управленческих решений [24-28].

Анализ работ по управлению ИТКС СН [12-22] показал, что в основе процесса подготовки управленческих решений лежат действия по моделированию значений интересующих исследователя характеристик ИТКС для заданного набора исходных данных и сравнение результатов моделирования с заданными критериями в целях определения направления управленческих действий.

Допустим, что математические модели определения частных показателей эффективности функционирования ИТКС СН известны. Тогда, в интересах моделирования характеристик защищенности ИТКС СН в условиях конфликта

требуется разработать метод разработки управленческих решений по управлению структурой ИТКС и параметрами ее элементов. В данном случае, в первую очередь, требуется определить перечень исходных данных, на основе которых должно проводиться моделирование влияния изменения значений характеристик защищенности ИТКС СН в условиях информационного конфликта.

Определить состав конфликтующих систем можно аналогично подходу, представленному в работах [12, 28-31], основанных на рассмотрении описательных моделей информационного конфликта, созданных на основе теорий конфликта и системного анализа. При этом, при описании составляющих элементов конфликтующих систем применяется математический аппарат теории множеств.

Ввиду того, что задачей статьи является разработка метода повышения защиты ИТКС СН в условиях информационного конфликта, использование математических методов теории конфликта в полной мере не требуется, в данной работе теория конфликта используется с целью определения составляющих антагонистических систем, влияющих на течение конфликта и определения целей конфликтующих сторон в конфликте.

В работе [4] показано, что, как правило, воздействие нападающей стороной на защищающейся объект является следствием вскрытия объекта системой разведки нападающей стороны. Поэтому, основной упор в данной работе сделан на управлении параметрами ИТКС СН защищающейся стороны в целях повышения ее защищенности от разведки нападающей стороны, а также, в силу стохастичности результатов ведения разведки, нивелирования результатов дестабилизирующих действий нападающей стороны на ИТКС СН. Требуется на основе использования результатов моделирования текущих и прогнозируемых частных показателей качества функционирования ИТКС СН разработать метод управления структурой ИТКС и параметрами ее элементов в интересах повышения защиты от разведки нападающей стороны. Данный метод должен описывать процессы, протекающие в системе управления ИТКС СН, основываясь на теории управления, и по своей сути являться моделью функционирования системы управления.

Существуют различные способы представления (описания) и реализации математических моделей [32, 33]: концептуальные или содержательные, физические или материальные, математические или абстрактные, программные (алгоритмические, компьютерные). Учитывая опыт предыдущих исследований по созданию методов и способов управления сложными объектами [21, 22, 26-28], к которым относится и ИТКС СН, наиболее удобным способом описания процесса управления является алгоритмический, так как он в наиболее доступной и наглядной форме отражает логику действий системы управления по управлению сложным объектом, а также, при этом, в отличии от абстрактного описания системы управления обладает наибольшей практической ценностью.

Ввиду того, что процесс управления ИТКС СН связан с выработкой управленческих решений, которые должны приниматься с учетом складывающейся обстановки и наличия ресурсов, то разрабатываемый метод должен содержать действия выработки решений по повышению защищенности от развед-

ки, а также оценки эффективности разработанных решений по заданному критерию. В данном случае, на первом этапе требуется рассмотреть все возможные комбинации действий по повышению РЗ, здесь целесообразно использовать методы комбинаторики. Для определения значений показателей РЗ и качества функционирования элементов ИТКС СН, а также влияния каждого набора действий на них требуется использовать методы моделирования. Выбор предпочтительного варианта возможен на основе применения методов теории оптимизации.

Учитывая проведенные выше рассуждения, последовательность действий по разработке метода защиты ИТКС СН в условиях конфликта и используемый теоретический базис можно представить схемой, изображенной на рис. 1. Таким образом, разрабатываемый метод базируется на использовании теорий конфликта, системного анализа, множеств, управления, оптимизации, моделирования и комбинаторики.

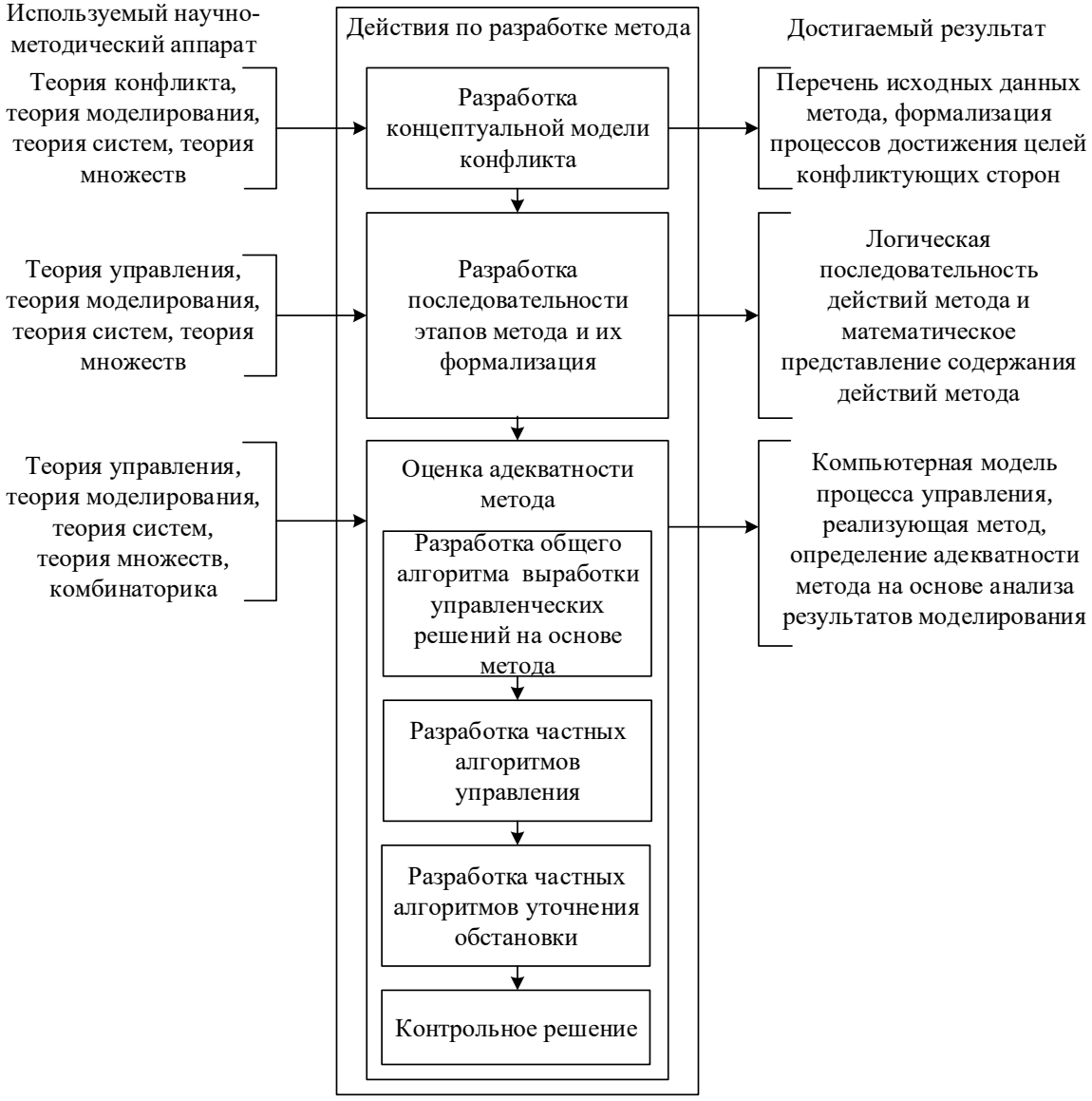

Рис. 1. Последовательность действий по разработке метода защиты ИТКС СН в условиях информационного конфликта

Концептуальная модель конфликта

Прежде чем перейти к разработке метода управления РЗ элементов ИТКС СН, требуется определить состав конфликтующих сторон и рассмотреть содержание конфликтной ситуации [34, 35].

В работе [12] представлено подробное описание концептуальной модели информационного конфликта двух организационно-технических систем – защищающейся и нападающей сторон. Данная модель представлена на рис. 2 (тонкие линии). Конфликтующими являются стороны S_1 и S_2. Сторона S_2 является нападающей стороной, сторона S_1 выступает защищающейся стороной.

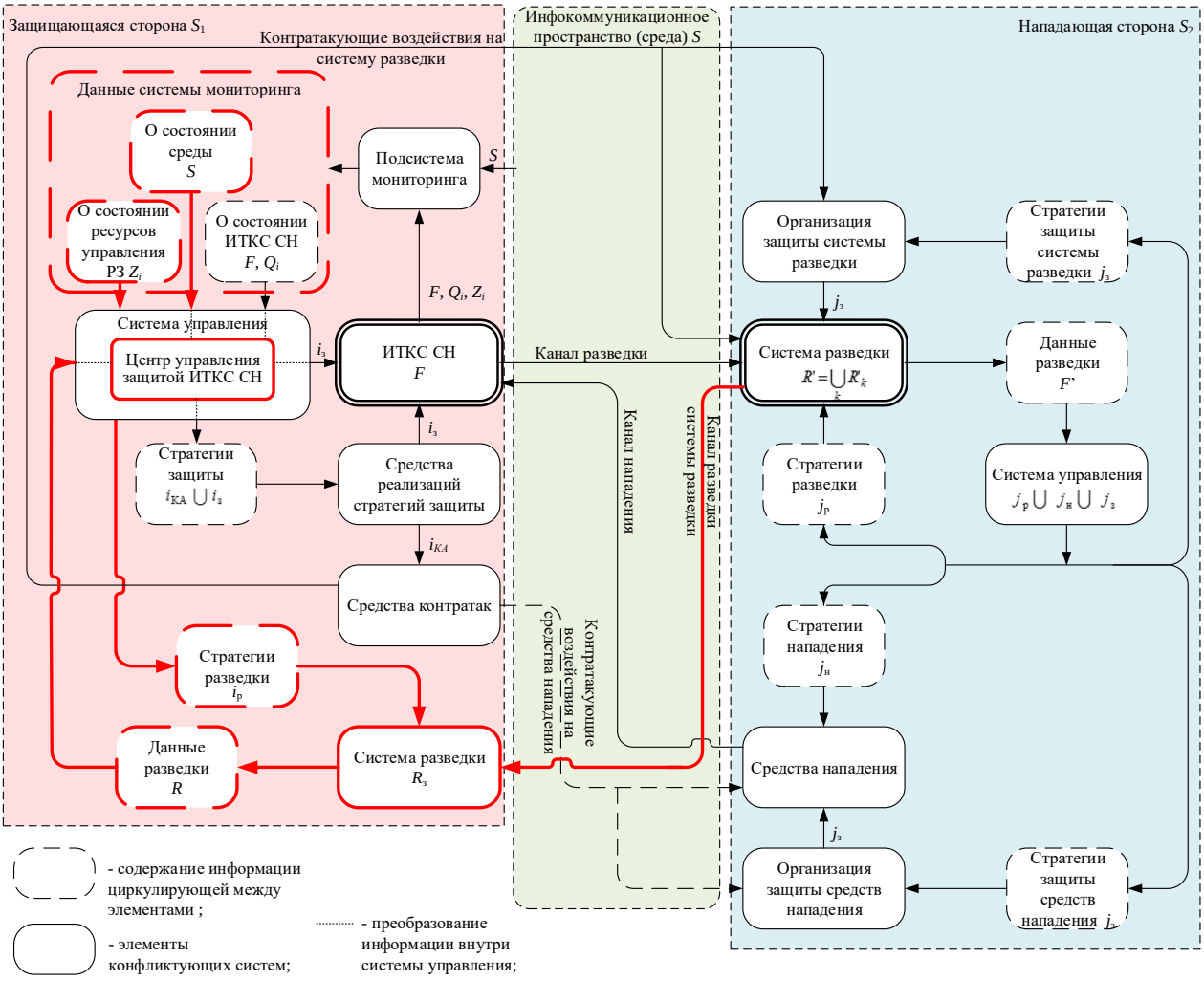

Рис. 2. Схема концептуальной модели информационного конфликта

В соответствии с задачей статьи, представленная в [12] схема доработана, добавлены дополнительные элементы на защищающейся стороне S_1 схемы информационного конфликта в части добавления системы разведки $R_з$ и центра управления защитой ИТКС СН, являющегося элементом системы управления, и расширения функций подсистемы мониторинга в части сбора и уточнения данных о состоянии среды S и наличия ресурсов по управлению РЗ Z_i (выделены красной линией, на рис. 2). Внесенные изменения в части добавления системы разведки защищающейся стороны позволяют сделать конфликтующие стороны

симметричными друг другу, что в большей степени соответствует действительности. Также, данные изменения позволяют учесть при моделировании конфликта возможные изменения в составе и режимах работы системы разведки нападающей стороны, необходимые для адекватной оценки временных и вероятностных параметров РЗ элементов сети связи [4, 22, 36]. Расширение функций мониторинга обосновывается необходимостью учета при планировании функционирования элемента ИТКС СН наличия ресурсов Z_i по управлению РЗ и значений параметров окружающей среды S.

В моделируемом конфликте (рис. 2) основными конфликтующими системами являются с защищающейся стороны – ИТКС СН, характеризуемая множеством F, с нападающей стороны – система разведки, характеризуемая множеством R'. Конфликтующие системы действуют не самостоятельно, а в составе конфликтующих систем более высшего порядка – системы управления и системы нападения на ИТКС СН, с защищающейся S_1 и нападающей S_2 сторон, соответственно.

С учетом введенных дополнений в концептуальную модель информационного конфликта (рис. 2), пояснений и ограничений, описанных выше, динамика развития конфликтна будет следующей.

Нападающая сторона ведет разведку ИТКС СН F защищающейся стороны, состоящей из определенного количества элементов в количестве $N_{\text{ИТКС}}$, где каждый элемент характеризуется множеством O_i. Параметры o_{i,m_i} каждого элемента ИТКС СН O_i в фиксированный момент времени обладают определенной степенью доступности средствам системы разведки нападающей стороны [4, 7, 16, 22, 36, 37], из-за чего полученные системой разведки измерения параметров характеризуются некоторой ошибкой измерения. Вскрытие ИТКС СН системой разведки характеризуется степенью определения структуры ИТКС, что достигается вскрытием количества, состава и назначения элементов ИТКС по их признакам, а также определением взаимосвязей между элементами ИТКС [38]. Математически процесс вскрытия можно представить следующими выражениями:

$$X: <F, S, R', t> \rightarrow F^*, \quad (2)$$

где: X – искомое преобразование, характеризующее работу системы разведки; F^* – результат работы системы разведки нападающей стороны по вскрытию ИТКС СН (множество, характеризующее ИТКС СН защищающейся стороны, полученное системой разведки),

$$F^* = \bigcup_{i=1}^{N^*_{\text{ИТКС}}} O^*_i, \quad (3)$$

где O^*_i – результат работы системы разведки нападающей стороны по вскрытию i-го элемента ИТКС СН (множество, характеризующее i-й элемент ИТКС СН защищающейся стороны, полученное системой разведки),

$$O^*_i = \{o^*_{i,m_i}\}, m_i=1, \ldots, M_i, \quad (4)$$

где o^*_{i,m_i} – значение m_i-го параметра i-го элемента ИТКС СН, измеренное системой разведки нападающей стороны,

$$o^*_{i,m_i} = o_{i,m_i} \pm \varepsilon_{i,m_i}, \quad (5)$$

где ε_{i,m_i} – ошибка измерения m_i-го параметра i-го элемента ИТКС СН.

Множество, характеризующее ошибки измерения параметров элемента ИТКС СН, можно определить следующим выражением:

$$E_i = \{\left|\varepsilon_{i,m_i}\right|\}. \quad (6)$$

Данные разведки, полученные средствами системы разведки F^*, поступают в вышестоящую систему – систему управления нападающей стороны, в которой вырабатываются решения по стратегиям [12]: нападения на ИТКС СН средствами нападения $j_н$, ведения разведки системой разведки $j_р$, защиты системы разведки и средств нападения $j_з$. В соответствии с выработанными стратегиями средства нападения и система разведки отрабатывают атакующие и защитные действия.

Адекватность стратегий действий атакующей стороны, характеризуется уровнем достоверности и своевременности разведывательной информации, характеризуемой выражением

$$F^* \approx F \mid t \le t_{\text{треб.}}, \quad (7)$$

где $t_{\text{треб.}}$ – предельное время вскрытия ИТКС СН, в течение которого разведывательные данные остаются актуальными; ≈ – символ, характеризующий взаимное попарное соответствие (равенство) элементов множеств F^* и F, т.е. $f_i \approx f^*_i$.

Из выражений (3) и (7) следует, что

$$O^*_i \approx O_i. \quad (8)$$

Из выражения (8) следует, что

$$o^*_{i,m_i} \approx o_{i,m_i}. \quad (9)$$

Тогда, из выражения (5) следует, что выполнение выражения (9) возможно при условии

$$\varepsilon_{i,m_i} \to 0. \quad (10)$$

В соответствии с работами [39, 40], посвященными распознаванию объектов, вскрытие элемента ИТКС СН характеризуется степенью совпадения измеренных значений параметров искомым значениям, т.е. выражение (10) эквивалентно выражению

$$\varepsilon_{i,m_i} \to \varepsilon_{\min i,m_i}, \quad (11)$$

где $\varepsilon_{\min i,m_i}$ – минимальное значение погрешности измерения, при котором значение искомого параметра однозначно идентифицируется.

Таким образом, первичной целью системы разведки нападающей стороны в рассматриваемом конфликте является получение оценок параметров элементов ИТКС СН, отвечающих выражению (5) при условии (11).

На защищающейся стороне функционирует ИТКС СН F, разведку которой проводит нападающая сторона R'. Управляет функционированием ИТКС СН система управления, которая задает целевые установки функционирования и критерии эффективного функционирования ИТКС $Q_{\text{доп.}i}$, собирает данные от соответствующих подсистем: мониторинга состояния ИТКС СН (множества F и Q_i) и окружающей среды S, мониторинга наличия ресурсов по повышению защиты от разведки Z_i и системы разведки защищающейся стороны о системе

разведки нападающей стороны *R*. Математически данные процессы можно представить выражениями:

$$Y_S: <S, t> \rightarrow S_{\text{тек.}}, \quad (12)$$

где Y_S – искомое преобразование, характеризующее работу системы мониторинга и прогнозирования состояния окружающей среды; $S_{\text{тек.}}$ – текущее значение множества, характеризующего состояние окружающей среды, определенное системой мониторинга;

$$Y_F: <F, Q_i, t> \rightarrow <F_{\text{тек.}}, Q_{i.\text{тек.}}> \mid \forall i, i = 1,..., N_{ИТКС}, \quad (13)$$

где Y_F – искомое преобразование, характеризующее работу системы мониторинга и прогнозирования состояния ИТКС СН; $F_{\text{тек.}}$ – текущее значение множества, характеризующего состояние ИТКС СН, определенное системой мониторинга; $Q_{i.\text{тек}}$ – текущее значение множества, характеризующего значение показателей качества функционирования элементов ИТКС СН, определенное системой мониторинга;

$$Y_Z: <Z_i, t> \rightarrow Z_{\text{тек}.i}, \quad (14)$$

где Y_Z – искомое преобразование, характеризующее работу системы мониторинга наличия ресурсов по управлению РЗ элементов ИТКС СН;

$$Y_R: <R_з, S, R', t> \rightarrow R, \quad (15)$$

где Y_R – искомое преобразование, характеризующее работу системы разведки защищающейся стороны.

Система управления имеет в своем составе функциональный модуль управления защитой ИТКС СН – центр управления защитой ИТКС СН, отвечающий за обеспечение защиты ИТКС СН от разведки стороны S_2. Центр управления защитой ИТКС СН имеет доступ к информации, хранящейся в системе управления в соответствии с установленным уровнем доступа, на основе данной информации о текущем состоянии множеств $F_{\text{тек.}}$, $Q_{i.\text{тек.}}$, $Z_{\text{тек}.i}$, R, $S_{\text{тек.}}$ в нем проводится моделирование значений РЗ элементов ИТКС СН, разрабатываются варианты решений по обеспечению защиты ИТКС СН от разведки нападающей стороны $Pr_{\text{действ}.i}$ и определяются оптимальные из них:

$$Y: <F_{\text{тек.}}, Q_{i.\text{тек.}}, Z_{\text{тек}.i}, R, S_{\text{тек.}}, t> \rightarrow opt\{Pr_{\text{действ}.i}\}, \quad (16)$$

где Y – искомое преобразование, характеризующее работу центра управления защитой ИТКС СН.

На основе полученных данных от системы мониторинга, разведки и центра управления защитой ИТКС, система управления вырабатывает стратегии: защиты, содержащие управление активными и пассивными методами защиты ИТКС СН от систем разведки и средств нападения нападающей стороны $i_з$, отражающиеся в плане функционирования ИТКС СН; контратакующих действий $i_{КА}$; разведки для системы разведки защищающейся стороны $i_р$. Данные стратегии доводятся до соответствующих исполнительных подсистем. Средства контратак осуществляют воздействия на средства нападения и разведки системы разведки нападающей стороны. Результаты данных воздействий фиксируются системой разведки защищающейся стороны и передаются в систему управления в виде уточненных данных о системе разведки атакующей стороны *R*.

Из выражений (12) – (16) следует, что точность управления определяется корректностью исходных данных и действиями по их преобразованию. Очевидно, что все действия системы защиты ИТКС СН должны быть направлены на невыполнение условия (11), или на выполнение обратного условия, заданного выражением:

$$\varepsilon_{i,m_i} \to \max \mid \max >> \varepsilon_{\min i,m_i}. \quad (17)$$

Таким образом, суть информационного конфликта между системой управления защищающейся стороны S_1 и системой нападения на ИТКС СН нападающей стороны S_2 можно выразить, как противоборство двух стратегий $i_з \cup i_{КА} \cup i_р$ и $j_н \cup j_р \cup j_з$. Основой адекватности каждой стратегии являются достоверные исходные данные и корректность действий по их преобразованию при выработке стратегий. Для системы нападения на ИТКС СН основными исходными данными являются данные системы разведки (2). Для системы управления защищающейся стороны в части организации защиты ИТКС СН основными исходными данными является результат работы центра управления защитой ИТКС СН (16).

Отсюда следует, что в основа успешности исхода информационного конфликта вышестоящих систем (системы управления защищающейся стороны и системы нападения на ИТКС СН) является успешность исхода информационного конфликта системы разведки нападающей стороны, стремящейся выполнить условие (11), и ИТКС СН, управляемой системой управления защитой ИТКС СН, стремящейся выполнить выражение (17).

В выражениях (11) и (17) в качестве успешности результата работы системы разведки и защиты ИТКС СН выступает ошибка измерения параметров, характеризующих элемент ИТКС СН. Значения данных величин на практике являются практически непредсказуемыми, что не позволяет их использовать в качестве управляемого параметра при формировании действий по защите элементов ИТКС СН. В работах по защите объектов от систем технической разведки [4-7] в качестве параметра оценки возможностей разведки используют подходы теории вероятностей и оперируют вероятностью вскрытия объекта $P_{вскр.}$. Показать взаимосвязь ошибки измерения и вероятности вскрытия объекта можно с помощью теоремы, представленной ниже.

Теорема. Пусть при ведении разведки объекта O_i, характеризующегося параметрами o_1, o_2, o_3, ..., o_N, где N – количество параметров, существует такой набор случайных измерений параметров средствами и комплексами разведки O^*_i, характеризующийся параметрами o^*_1, o^*_2, o^*_3, ..., o^*_N. Требуется доказать, что существует такой набор измерений O^*_i, который с высокой вероятностью позволяет вскрыть объект разведки, т. е. имеет место быть равенство вида (8).

Доказательство. Доказательство проведем в два этапа. На первом этапе докажем возможность существования набора значений O^*_i, удовлетворяющего выражению (8). На втором этапе покажем, что набор значений O^*_i, позволяет вскрыть объект O_i с высокой вероятностью.

1. Пусть имеется объект разведки O_i, характеризующийся параметрами o_1, o_2, o_3, ..., o_N, т.е. объект O_i однозначно определяется многомерным вектором

$\overrightarrow{O_i}(o_1, o_2, ..., o_N)$, тогда результат измерений параметров объекта O_i также является многомерным вектором $\overrightarrow{O^*_i}(o^*_1, o^*_2, ..., o^*_N)$, в общем случае результат измерения каждого параметра носит случайный характер, т.е. в общем случае $o^*_n \neq o_n, \ \forall n, n = 1, ..., N$.

Определить ошибку измерения параметров объекта O_i можно на основе теории векторного исчисления [41]. Имеем следующее выражение для разности двух векторов:

$$\vec{E} = \overrightarrow{O_i} - \overrightarrow{O^*_i} = (o_1 - o^*_1, o_2 - o^*_2, ..., o_N - o^*_N) = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_N). \quad (18)$$

Известно, что разность двух одинаковых векторов есть нулевой вектор, следовательно при $\overrightarrow{O_i} \approx \overrightarrow{O^*_i}$:

$$\vec{E} = (\varepsilon_1 \to 0, \varepsilon_2 \to 0, ..., \varepsilon_N \to 0) \approx \vec{0}, \quad (19)$$

а это и является условием существования равенства вида (8).

2. Из теории измерений [42] при проведении многократных измерений координаты вектора $\vec{E}$ приближаются к значениям среднеквадратических отклонений (СКО) измерений *n*-го параметра объекта O_i.

Примем, что плотность вероятности проведения измерений вектора $\overrightarrow{O_i}$ есть многомерная функция плотности распределения $f(o^*_1, o^*_2, o^*_3, ..., o^*_N)$, которая характеризует вероятность измерения всех параметров вектора $\overrightarrow{O_i}(o_1, o_2, ..., o_N)$ с СКО $\vec{E}(\varepsilon_1, \varepsilon_2, ..., \varepsilon_N)$, что и характеризует вероятностью вскрытия объекта разведки $P_{\text{вскр.}}$ (следует из первой части доказательства).

Тогда, если $\overrightarrow{O_i} \approx \overrightarrow{O^*_i}$, то $\vec{E} \to \vec{0}$ или ($\varepsilon_1 \to 0, \varepsilon_2 \to 0, \ldots, \varepsilon_N \to 0$), следовательно $f(o^*_1, o^*_2, ..., o^*_N) \to \max$, или $P_{\text{вскр.}} \to \max$.

Наглядно данные выводы можно продемонстрировать на примере частного случая измерения значения одного параметра.

Пусть плотность распределения измерения параметра $f(o^*_1)$ имеет нормальный закон распределения $f(o^*_1) = \frac{1}{\sqrt{2\pi} \cdot \varepsilon_1} \cdot e^{-\frac{(o^*_1 - o_1)^2}{2 \cdot \varepsilon_1^2}}$. Графики функций $f(o^*_1)$ представлены на рис. 3, из них нетрудно видеть, что наибольшая вероятность вскрытия объекта разведки при попадании измерения в диапазон примерно равный искомому параметру ($o_1^* \approx o_1$) достигается при минимальных значениях СКО измерения параметров объекта разведки.

Т.е., при выполнении выражения (8) вероятность вскрытия объекта O_i является максимальной, т.е.

$$P_{\text{вскр.}} = \int_{-\Delta}^{\Delta} f(o^*_1) do^*_1 \to \max, \text{ при } \varepsilon_1 \to 0, \quad (20)$$

где $P_{\text{вскр.}}$ – вероятность вскрытия объекта разведки. Следовательно, имеется возможность с высокой вероятностью вскрыть объект разведки.

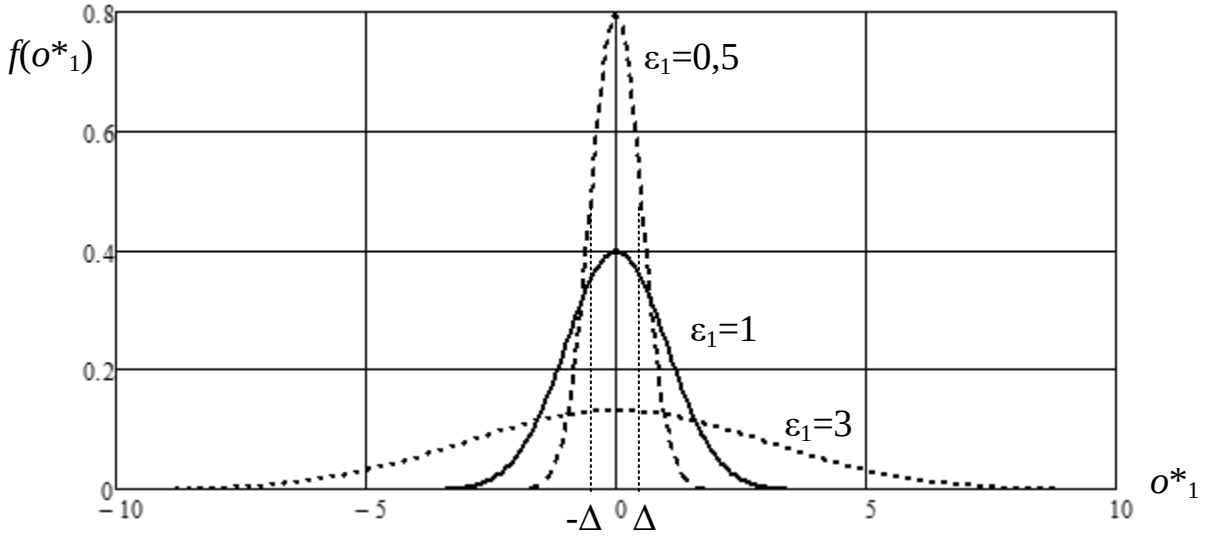

Рис. 3. Плотность распределения вероятности одного параметра объекта разведки при различных СКО измерений

Из выражения (20) следует, что ошибка измерения параметров элемента ИТКС СН, определяемая из выражения (5), находится в обратной зависимости с вероятностью вскрытия элемента ИТКС СН. Таким образом, в качестве управляемого параметра при реализации мер по защите ИТКС СН допустимо использовать вероятность вскрытия элемента ИТКС. То есть, эквивалентом выражениям (11) и (17) будут выступать выражения относительно $P_{\text{вскр.}}$:

– система разведки:

$$\varepsilon_{i,m_i} \to \varepsilon_{\min i,m_i} \Rightarrow P_{\text{вскр.}i} \to P_{\text{вскр.max}} \Rightarrow P_{\text{вскр.}i} > P_{\text{вскр.зад.}i}; \quad (21)$$

– ИТКС СН:

$$\varepsilon_{i,m_i} \to \max \Rightarrow P_{\text{вскр.}i} \to P_{\text{вскр.min}} \Rightarrow P_{\text{вскр.}i} \le P_{\text{вскр.зад.}i}, \quad (22)$$

или эквивалентно с учетом $P_{\text{вскр.}i}=1-P_{\text{РЗ }i}$,

$$P_{\text{РЗ }i} \ge P_{\text{РЗ зад.}i}. \quad (23)$$

Выражения (22) и (23) являются условием достижения успешного исхода информационного конфликта со стороны ИТКС СН, при условии, что оно выполняется для всех элементов ИТКС СН, что подтверждает справедливость выражения (1).

В рассматриваемом информационном конфликте между системой разведки *R*’ и ИТКС СН *F* учет возможных воздействий защищающейся стороны средствами контратак на нападающую сторону, а также воздействия атакующей стороны на ИТКС СН, средства разведки защищающейся стороны и средства контратак являются ограничениями данного конфликта. Данные ограничения являются справедливыми, так как ни система разведки ни ИТКС СН не являются средствами нападения и контратак. Данные средства являются участниками конфликта более высокого уровня. Однако, результаты двухсторонних деструктивных воздействий и возможность наращивания системы разведки атакующей стороной учитываются в процессе обновления данных поступающих от соответствующих подсистем мониторинга и разведки защищающейся стороны.

Метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта

Анализ работ по динамическому управлению системами [20-30, 43] показал, что адаптация к условиям изменения обстановки достигается на основе итерационного выполнения процедур: оценки условий и результатов функционирования управляемой системы; прогноза изменения условий и результатов функционирования управляемой системы; измерений условий функционирования и результатов функционирования управляемой системы. При чем, точность адаптации повышается с уменьшением длительности периода цикла управления [44]. Перечисленные процедуры характеризуют три основных метода управления системами – управление по возмущениям, управление по программе, управление по состоянию [24].

Осуществление способов управления по состоянию управляемого объекта в случае управления защитой ИТКС СН от разведки на основе прямого измерения показателей защищенности практически не представляется возможным по причине того, что защищенность от разведки оценивается вероятностными показателями. Кроме этого, защищенность от разведки является интегральной характеристикой, зависящей от нескольких составляющих – параметров и режимов функционирования объекта и системы разведки, окружающего фона (уровень помех, климатические, физико-географические условия), окружающего признакового фона [4, 22, 38]. Поэтому, показатели защитой ИТКС СН от разведки могут контролироваться косвенно расчетным методом на основе прямого измерения значений параметров, составляющих влияющих на РЗ.

Управление защитой элементов ИТКС СН от разведки по программе может быть реализовано на основе прогноза изменения показателей защищенности, полученного путем моделирования зависимости показателей защищенности элементов ИТКС СН для заданных условий обстановки на основе работ [38, 45-51], а также других в данной предметной области.

Из-за того, что реально определить абсолютное текущее значение показателей защищенности объекта от разведки в определенный момент времени во время конфликта невозможно ввиду стохастичности и многофакторности процесса ведения разведки, то, возможны определенные воздействия на элементы ИТКС, которые будут осуществлены вопреки прогноза изменения защищенности элементов ИТКС СН, полученного методами теории вероятностей. Воздействия нападающей стороны на элементы ИТКС отражаются на качестве функционирования ИТКС по назначению, приводя к ухудшению характеристик функционирующей ИТКС. Поэтому, в методе управления требуется учитывать возможные отклонения всей совокупности показателей качества функционирования ИТКС СН, а не только показатели защищенности от разведки.

Следовательно, управление разведывательной защищенностью элементов ИТКС СН по возмущениям может быть реализовано на основе измерения состояния параметров и режимов функционирования системы разведки, окружающего фона и окружающего признакового фона, а также на основе изменения качества функционирования линий связи ИТКС СН, исходящих от объекта раз-

ведки. Снижение качества функционирования ИТКС СН требует реализации корректирующих действий по парированию результатов воздействия, что приведет к изменению параметров функционирования элемента ИТКС. Определенное несоответствие параметров, составляющих защищенности от разведки предыдущим значениям потребует проведение моделирования показателей защищенности для текущих значений и коррекцию прогноза их изменения, которые станут основой для управления по состоянию объекта и управления по программе. Кроме этого, с учетом специфики функционирования ИТКС СН, функционирующих в интересах систем управления СН, которые формируют целевые установки функционирования ИТКС и ее элементов, в методе управления защищенностью элементов ИТКС должны учитываться возможные изменения целевой установки, поступающие от вышестоящей системы.

Таким образом, метод управления защищенностью элементов ИТКС СН от разведки должен содержать:

1. Функции планирования функционирования ИТКС, отражающие процедуры:

а) первичного планирования развертывания и функционирования ИТКС СН с учетом прогноза развития обстановки и требований к функционированию элементов ИТКС СН:

$$M_1 :< S_1, S_2, S, Q_{\text{доп}.i} >\!\!\rightarrow F, \tag{24}$$

где M_1 – символ искомого преобразования, характеризующий процесс разработки первичного плана развертывания и функционирования ИТКС СН;

б) оценки РЗ элементов ИТКС СН, функционирующих по заданному плану, на предмет выполнения заданных требований:

$$M_2 :< O_i, F_i, S, R >\!\!\rightarrow P_{\text{РЗ}i}(t) \,|\, t \le t_{\text{зад}.i}, \text{ для } \forall i, i = 1,..., N_{ИТКС}; \tag{25}$$

где M_2 – символ искомого преобразования, характеризующего научно-методический аппарат по оценке РЗ элементов ИТКС СН.

При выполнении условия

$$P_{\text{РЗ}i}(t \le t_{\text{зад}.i}) \ge P_{\text{РЗзад}.i}, \text{ для } \forall i, i = 1,..., N_{ИТКС} \tag{26}$$

первичный план развертывания и функционирования считается соответствующим требованиям по РЗ. В случае невыполнения условия (26) план считается несоответствующим требованиям по РЗ, что свидетельствует о необходимости принятия дополнительных мер по РЗ в элементе ИТКС СН или корректировке первичного плана развертывания и функционирования ИТКС СН.

в) корректировке плана развертывания и функционирования на предмет выполнения требований по РЗ элементов ИТКС СН и качества функционирования элементов ИТКС СН по назначению. Для всех элементов ИТКС СН, для которых не выполняется условие (26) определяется множество, содержащее наборы действий по повышению РЗ

$$M_3 :< O_i, F_i, S, R, Z_i, W_i >\!\!\rightarrow Pr_{\text{действ}.i} \,\big|\, P_{\text{РЗ}i}(t \le t_{\text{зад}.i}) \ge P_{\text{РЗзад}.i}, \tag{27}$$

где M_3 – символ искомого преобразования, характеризующего научно-методический аппарат по выработке множества, содержащего варианты наборов действий по повышению РЗ.

Если

$$Pr_{\text{действ}.i}=\varnothing, \quad (28)$$

то это означает, что при имеющихся ресурсах Z_i по повышению РЗ не найдено ни одного набора действий по повышению РЗ i-го элемента ИТКС СН, что свидетельствует о невозможности выполнения требований по РЗ в заданных условиях и необходимости пополнения ресурсов и/или корректировке требований по РЗ в сторону снижения, либо корректировке первичного плана развертывания и функционирования ИТКС СН.

Если, условие (28) не выполняется, то это означает, что определены наборы действий по повышению РЗ i-го элемента ИТКС СН. В данном случае необходимо оценить качество функционирования элемента ИТКС СН на предмет выполнения требований $Q_{\text{доп}.i}$ с учетом применения найденных наборов действий по повышению РЗ $Pr_{\text{действ}.i}$.

Проводится моделирование значений показателей качества функционирования элементов ИТКС СН по назначению

$$M_4 :< O_i, F_i, S, Pr_{\text{действ}.i} >\rightarrow Q_i, \quad (29)$$

где M_4 – символ искомого преобразования, характеризующего действия по моделированию значений показателей качества функционирования элемента ИТКС СН [5, 52].

Запоминаются элементы множества $Pr_{\text{действ}.i}$, для которых выполняется условие

$$q_{i,g_i} \geq q_{\text{доп}.i,g_i} \mid \forall g_i,\ g_i = 1,...,G_i. \quad (30)$$

Если, элементы множества $Pr_{\text{действ}.i}$, для которых выполняется условие (30) не определены, то это свидетельствует о том, что достижение заданных требований по РЗ в данном элементе без нарушения качества функционирования элемента ИТКС СН не представляется возможным. В данном случае необходимо, либо корректировать требования по РЗ в сторону снижения, либо изменять первичный план развертывания и функционирования ИТКС СН.

Если, количество элементов множества $Pr_{\text{действ}.i}$, для которых выполняется условие (30), больше одного, переходят к выбору из них оптимального набора действий по повышению РЗ элемента ИТКС СН на основе заданного критерия оптимальности. Для этого, вычисляются элементы множеств $T_{\text{реализ}.i}$ и $C_{\text{реализ}.i}$, для соответствующих элементов множества $Pr_{\text{действ}.i}$:

1) определяются значения временных затрат по выражениям:

– для последовательного метода реализации действий по повышению РЗ

$$t_{\text{реализ}.h_i\ v_1,v_2,...,v_{h_i}} = tw_{\text{реализ}.v_1} + tw_{\text{реализ}.v_2} + ... + tw_{\text{реализ}.v_{h_i}}; \quad (31)$$

– для параллельного метода реализации действий по повышению РЗ

$$t_{\text{реализ}.h_i\ v_1,v_2,...,v_{h_i}} = \max(tw_{\text{реализ}.v_1}, tw_{\text{реализ}.v_2},..., tw_{\text{реализ}.v_{h_i}}); \quad (32)$$

и материальных затрат по выражению

$$c_{\text{реализ}.h_i\ v_1,v_2,...,v_{h_i}} = cw_{\text{реализ}.v_1} + cw_{\text{реализ}.v_2} + ... + cw_{\text{реализ}.v_{h_i}}. \quad (33)$$

2) выстраивают вариационные ряды по временным и материальным затратам, вычисленным по выражениям (31) – (33), для всех элементов множества $Pr_{\text{действ.}i}$, для которых выполняется условие (30);

3) по вариационным рядам определяют оптимальный вариант повышения РЗ элемента ИТКС СН, по одному из критериев выражения (1) либо их комбинации

$$opt < T_{\text{реализ.}i}, C_{\text{реализ.}i} > \rightarrow opt < Pr_{\text{действ.}i} > . \quad (34)$$

При этом, могут быть использованы различные методы оптимизации [53-58].

Оптимальный вариант действий, определенный в соответствии с (34), вносится в план развертывания и функционирования ИТКС СН.

2. Функции оперативного управления ИТКС СН, содержащие процедуры управления:

а) с учетом оценки изменения РЗ элементов ИТКС СН в соответствии с текущими значениями множеств O_i, R, S, F_i.

От соответствующих подсистемах (рис. 2) системы управления принимается обновленная информация по множествам F, S, R.

В случае соответствия имеющейся текущей в центре управления РЗ ИТКС СН и поступившей от соответствующих подсистем информации об обновленных множествах

$$F \approx F_{\text{тек.}}; R \approx R_{\text{тек.}}; S \approx S_{\text{тек.}}, \quad (35)$$

корректирующих действий по управлению ИТКС СН не предпринимается. В данном случае элементы ИТКС СН продолжают функционировать в соответствии с ранее имеющимся планом.

В случае невыполнения условий (35), определяются показатели РЗ с учетом примененных наборов действий по повышению РЗ и обновленных исходных данных в каждом элементе ИТКС СН:

$$M_5 :< O_i, F_i, S, R, Pr_{\text{действ.}i} > \rightarrow P_{\text{РЗ}i}(t) \big| t \le t_{\text{зад.}i} , \quad (36)$$

где M_5 – символ искомого преобразования, характеризующего научно-методический аппарат по оценке РЗ элементов ИТКС СН с учетом примененных действий по повышению РЗ.

Проводится сравнение полученного значения показателя РЗ с полученным на предыдущем цикле управления РЗ ИТКС СН при $t=t_{\text{зад.}i}$:

– при

$$P_{\text{РЗ}i}(t_{\text{зад.}i}) \ge P_{\text{РЗ}i\ \text{пред.}}(t_{\text{зад.}i}), \quad (37)$$

где $P_{\text{РЗ}i\ \text{пред.}}(t_{\text{зад.}i})$ – значение вероятности разведывательной защищенности i-го элемента ИТКС СН, определенное на предыдущем шаге цикла управления; элементы ИТКС СН продолжают функционировать в соответствии с ранее имеющимся планом, т.е. $t_{\text{зад.}i}$ остается неизменным. Либо, возможен вариант увеличения $t_{\text{зад.}i}$, которое можно определить из уравнения

$$P_{\text{РЗ}i}(t_{\text{зад.}i}) = P_{\text{РЗ}i\ \text{зад.}}; \quad (38)$$

– при невыполнении условия (37) проверяется выполнение условия

$$P_{\text{РЗ}i}(t + t_{\text{сверт.}i}) \ge P_{\text{РЗ}i\ \text{зад.}}, \quad (39)$$

где t – текущее значение времени; $t_{\text{сверт.}i}$ – время свертывания элемента ИТК СН для перемещения.

При выполнении условия (39) определяется новое предельно допустимое время нахождения элемента ИТКС СН в данном состоянии $t_{\text{зад.}i.}$ из выражения (38).

При невыполнении условия (39) предпринимаются немедленные меры по изменению состояния элемента ИТКС СН, для исключения возможного поражения средствами нападения нападающей стороны (рис. 2);

б) на основе значений множества Q. В процессе функционирования показатели качества функционирования элемента ИТКС СН по назначению постоянно контролируются системой мониторинга. В соответствии с текущим этапом функционирования ИТКС СН в конфликте приоритетными могут становиться те или иные показатели качества функционирования [5, 59–61]. Данная приоритетность устанавливается системой управления как вышестоящей системой

$$M_6 :< Q_i >\rightarrow Q_{\text{п.}i}, \tag{40}$$

где M_6 – символ искомого преобразования, характеризующего действия по выбору приоритетных показателей качества функционирования; $Q_{\text{п.}i}$ – множество приоритетных показателей качества функционирования. В общем случае $Q_{\text{п.}i} \approx Q_i$.

Данные подсистемы мониторинга состояния ИТКС СН в части определения качества функционирования сравниваются с заданными требованиями (30).

В случае выполнения условия (30) никаких действий по управлению элементом ИТКС СН не предпринимается. При невыполнении условия (30) проводятся действия по повышению показателя качества функционирования элемента ИТКС СН в части повышения значений параметра качества функционирования по назначению

$$M_7 :< O_i, F_i, S, Pr_{\text{действ}i} >\rightarrow q_{i,g_i} \left| q_{i,g_i} \geq q_{\text{доп}.i,g_i} \forall g_i, g_i = 1,...,G_i. \right., \tag{41}$$

где M_7 – символ искомого преобразования, характеризующего действия, приводящие к обеспечению значения показателя качества функционирования.

Выполнение действий (41) может привести к изменению множества F. Данное изменение будет учтено при управлении РЗ на следующем шаге цикла управления ИТКС СН.

в) на основе учета изменений условий развития конфликта с учетом прогноза, отличных от первоначального плана развертывания и функционирования (изменение целевой установки функционирования ИТКС СН). В процессе развития конфликта в конечном счете он может идти не по ранее намеченному плану, в данном случае ИТКС СН приходится адаптировать под изменения условий. Это эквивалентно процессу первичного планирования развертывания и функционирования ИТКС СН, моделируемому выражением (24) с последующими действиями, представленными выражениями (25) – (39).

3. Функции контроля функционирования ИТКС СН и складывающейся обстановки, содержащие процедуры:

а) контроля значений параметров элементов ИТКС СН на предмет соответствия заданным значениям для выполнения требований по РЗ и качеству функционирования (измерение множеств O_i, $\forall i, i = 1,..., N_{\text{ИТКС}}$.), а также качества функционирования элементов ИТКС СН, характеризуемого выражением (13);

б) контроля значений параметров окружающей среды (измерение множества S), характеризуемого выражением (12);

в) контроля наличия ресурсов по обеспечению РЗ элементов ИТКС СН, характеризуемого выражением (14);

г) добывания сведений о системе разведки нападающей стороны системой разведки защищающейся стороны, характеризуемого выражением (15).

Проверку адекватности метода предлагается провести путем моделирования и решения тестовой задачи, в соответствии с (рис. 1).

Алгоритм, реализующий метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта

Блок-схема алгоритма, реализующего метод защиты ИТКС СН в условиях информационного конфликта, представлена на рис. 4.

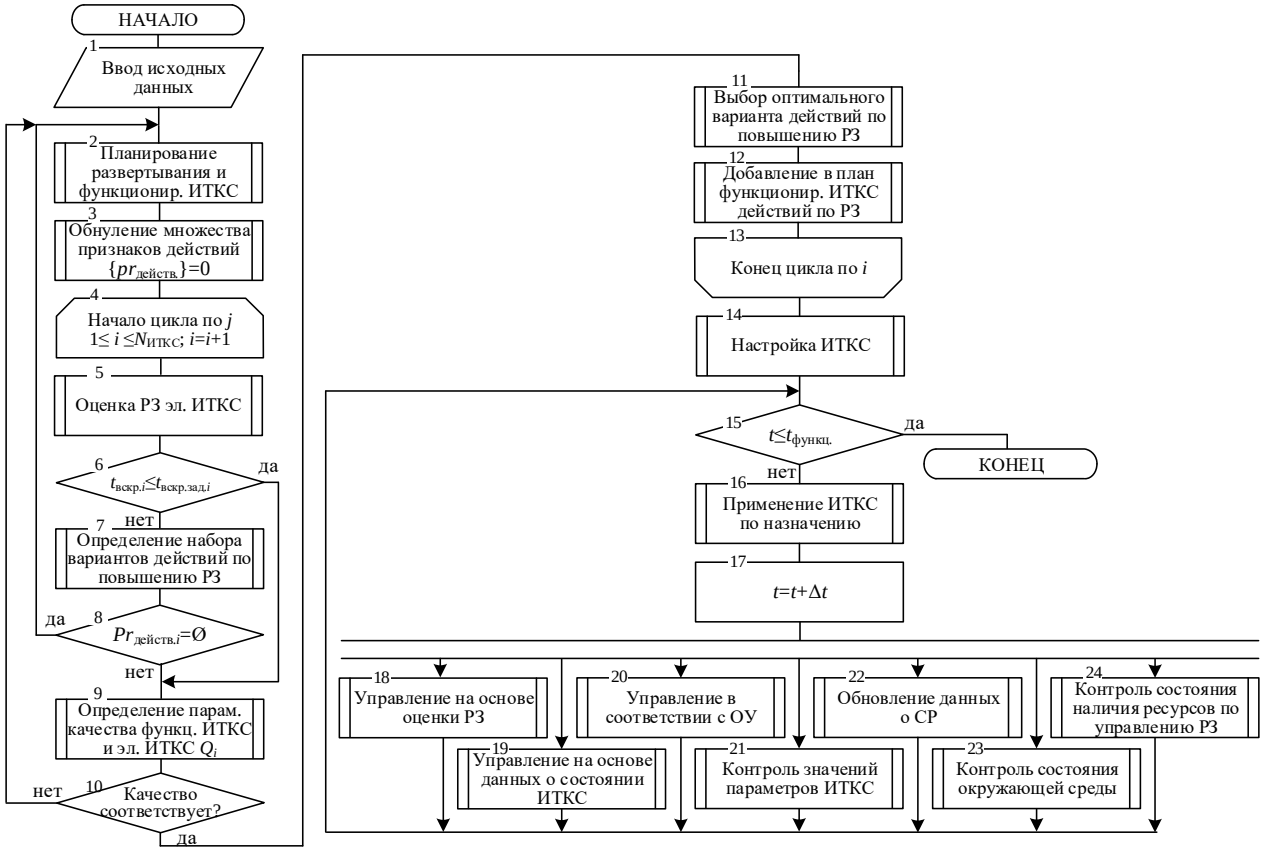

Рис. 4. Блок-схема алгоритма, реализующего метод защиты ИТКС СН в условиях информационного конфликта

Функции планирования функционирования ИТКС СН на основе динамического управления защищенностью

Блоки 1 – 13 рис. 4 реализуют подготовительный этапы планирования функционирования ИТКС СН и ее элементов.

На первоначальном этапе осуществляется ввод необходимых для планирования функционирования исходных данных (блок 1 рис. 4). Исходные данные содержат априорные сведения по множествам F; R; S; $\bigcup_{i=1}^{N_{\text{ИТКС}}} Z_i$; $\bigcup_{i=1}^{N_{\text{ИТКС}}} Q_{\text{доп}.i}$; $\bigcup_{i=1}^{N_{\text{ИТКС}}} W_i$; $P_{\text{вскр.доп}.i}$, i=1, …, $N_{\text{ИТКС}}$; $t_{\text{зад}.i}$; $tw_{\text{реализ}.k_i}$; $cw_{\text{реализ}.k_i}$; $t_{\text{функц}.}$.

В блоке 2 рис. 4 проводится первичное планирование развертывания и функционирования ИТКС СН с учетом прогноза развития конфликта (24), возможных действий сторон, которое включает разработку различных документов, схем, карт и т.п., в которых устанавливается последовательность, способы и время выполнения поставленных задач; проведение рекогносцировки (выезд на место предполагаемого развертывания элементов ИТКС, проведение измерений размеров площадок для развертывания антенн и аппаратных связи, изучение физико-географических условий (измерение глубины переправ); оценка состояния окружающей среды (климатических и помеховых условий функционирования ИТКС) и т. п.); проведение расчетов и разработка вариантов построения ИТКС [59, 60].

Сделав допущение о том, что практические мероприятия по рекогносцировке проведены, задачу планирования функционирования можно декомпозировать на следующие действия: разработка графа ИТКС, определение требований к линиям связи между элементами ИТКС, формирование состава элементов ИТКС из имеющихся средств связи, определение режимов работы средств связи элементов ИТКС. Данные действия отражаются путем задания значений элементов множества O_i, характеризующих режим работы каждого средства связи элемента ИТКС [47, 62].

В блоке 3 рис. 4 осуществляется обнуление множества $\{Pr_{\text{действ.}}\}$.

В блоке 4 рис. 4 организуется цикл по всем элементам ИТКС СН.

В блоке 5 рис. 4 проводится оценка РЗ элемента ИТКС, заключающаяся в определении зависимости $P_{\text{вскр.}}(t)$ для заданных условий обстановки, выражение (25). Зависимости $P_{\text{вскр.}}(t)$ определяются при помощи моделирования на основе работ [5, 19, 37, 45-51].

В блоке 6 рис. 4 проводится проверка выполнения критериев РЗ для i-го элемента ИТКС, выражение (26). Для чего по полученной зависимости $P_{\text{вскр.}}(t)$ находится корень уравнения

$$P_{\text{вскр.}}(t_{\text{вскр.}}) = P_{\text{вскр.доп}.i}. \quad (42)$$

Проверяется выполнение условие превышения значения корня уравнения (42) над заданным критерием по времени вскрытия элемента ИТКС

$$t_{\text{вскр.}} \geq t_{\text{зад}.i}. \quad (43)$$

В случае выполнения условия (43) осуществляется переход к блоку 11 рис. 4, в обратном случае осуществляется переход к блоку 7 рис. 4.

В блоке 7 рис. 4 осуществляется поиск возможных вариантов повышения РЗ *i*-го элемента ИТКС путем анализа возможных вариантов действий по повышению РЗ из множества доступных действий *Wi* для данного элемента ИТКС в количестве K_i. Варианты действий определяются по всему множеству возможных вариантов в количестве

$$N_{\text{вар}.i} = \sum_{r=1}^{K_i} C_{K_i}^{r}, \quad (44)$$

где: $C_{K_i}^{r}$ – количество сочетаний из K_i возможных действий по повышению РЗ элемента ИТКС по *r* действий [41].

Блок-схема алгоритма поиска возможных вариантов действий по повышению РЗ элемента ИТКС СН, реализующая выражение (27), представлена на рис. 5. Данный алгоритм представляет собой оценку различных вариантов наборов действий по повышению РЗ элемента ИТКС СН. Ввиду отсутствия прямой функциональной зависимости показателей РЗ от множества факторов, оказывающих влияние на нее, возможность использования широкого спектра имеющихся методов распределения ресурсов [53-56] является весьма затруднительным. Кроме этого, специфика каждого элемента ИТКС СН на практике не позволяет во время течения конфликта передать имеющиеся ресурсы по управлению РЗ одного элемента другому. Поэтому, группы вариантов, состоящих из 1, 2, …, K_i действий по повышению РЗ определяются путем перебора возможных вариантов действий по повышению РЗ в количестве равном выражению под знаком суммы (44) для каждого элемента. Для этого, последовательно выполняются циклы (блоки 7.1-7.6, 7.7-7.16, 7.17-7.30, 7.31-7.47, рис. 5), в которых осуществляется перебор всех возможных вариантов действий для соответствующего количества действий K_i. В каждом цикле для еще нереализованной группы действий осуществляется моделирование применения данной группы действий по повышению РЗ (блоки 7.2, 7.11, 7.24, 7.41, рис. 5), оценка РЗ при реализации данной группы действий (блоки 7.3, 7.12, 7.25, 7.42, рис. 5), проверка достаточности ее применения путем проверки выполнения условия (43) (блоки 7.4, 7.13, 7.26, 7.43, рис. 5).

При выполнении условия (43) в соответствующем цикле (блоки 7.4, 7.13, 7.26, 7.43, рис. 5) осуществляется установка соответствующего признака применения набора действий $Pr_{\text{действ.1 }k1}$, $Pr_{\text{действ.2 }k1,\ k2}$, $Pr_{\text{действ.}Ki\ k1,\ldots,kKi}$, $k_1 = 1,\ldots,\ K_i$; $k_2 = 1,\ldots,\ K_i$; …; $k_{Ki} = 1,\ldots,\ K_i$; (блоки 7.5, 7.14, 7.27, 7.44, рис. 5) в 1, затем осуществляется переход к анализу возможности применения следующего набора действий (блоки 7.6, 7.15, 7.28, 7.45, рис. 5). В случае невыполнения условия (43) в блоках (блоки 7.4, 7.13, 7.26, 7.43, рис. 5) переходят к анализу возможности применения следующего набора действий (блоки 7.6, 7.15, 7.28, 7.45, рис. 5).

Завершение последовательного выполнения всех циклов (блоки 7.1-7.6, 7.7-7.16, 7.17-7.30, 7.31-7.47, рис. 5) свидетельствует об окончании проверки возможности применения наборов действий по повышению РЗ и установлении признаков применения для всех наборов действий. Далее осуществляется переход к блоку 8 рис. 4.

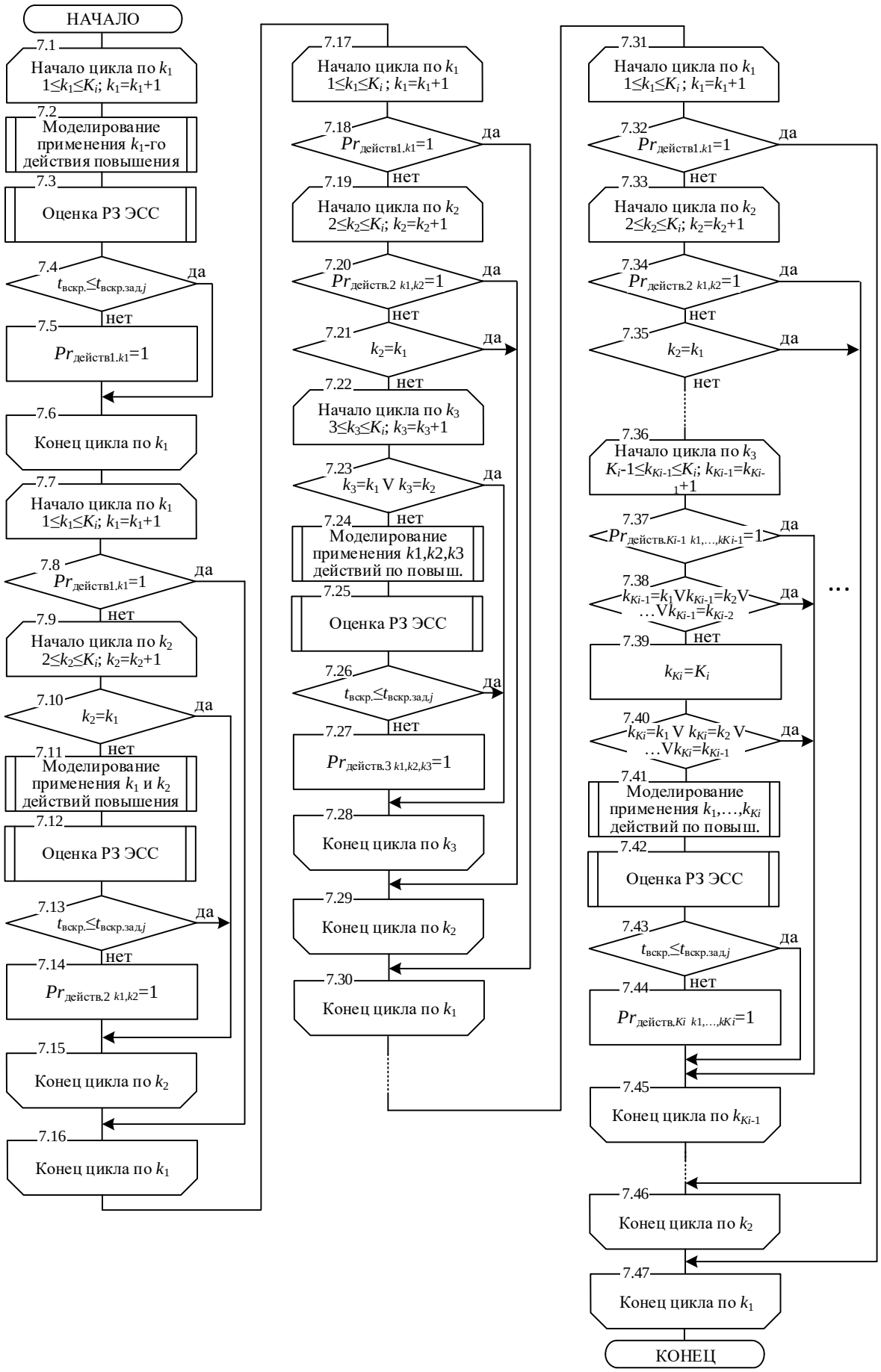

Рис. 5. Блок-схема алгоритма поиска возможных вариантов действий по повышению РЗ элемента ИТКС

В блоке 8 рис. 4 проверяют выполнение условия (28). В случае его выполнения условия, свидетельствующем об отсутствии вариантов повышения РЗ, переходят к блоку 2 рис. 4 для изменения плана функционирования ИТКС СН. В противном случае переходят к блоку 9 рис. 4.

В блоке 9 рис. 4 путем моделирования определяются значения параметров качества функционирования элемента ИТКС СН по назначению (множество Q_i), выражение (29).

В блоке 10 рис. 4 проверяется соответствие значения показателей качества функционирования ИТКС СН элементов множества Q_i заданным критериям $Q_{\text{доп}.i}$, выражение (30).

В случае несоответствия какого-либо параметра q_i заданному требованию $q_{\text{доп}.i}$ осуществляется переход к блоку 2 рис. 4 для изменения плана функционирования ИТКС СН. В обратном случае переходят к блоку 11 рис. 4.

В блоке 11 рис. 4 осуществляют выбор оптимального варианта действий по повышению РЗ элемента ИТКС СН по критерию эффективности, выражения (31) – (34).

Выбранный вариант действий по повышению РЗ для i-го элемента ИТКС СН вносят в план функционирования элемента ИТКС СН (блок 12 рис. 4).

Действия блоков 5-12 рис. 4 повторяют для всех элементов ИТКС СН. В блоке 13 рис. 4 проверяют условие окончания цикла, заданного блоком 4 рис. 4, после окончания цикла переходят к блоку 14 рис. 4.

В блоке 14 рис. 4 осуществляется развертывание и настройка ИТКС СН. Настройка ИТКС СН заключается в развертывании (реконфигурации) аппаратуры и техники связи, настройке аппаратуры и приведении ИТКС в работоспособное состояние.

Функции оперативного управления элементами ИТКС СН на основе данных мониторинга и с учетом прогноза складывающейся обстановки

В блоке 15 рис. 4 осуществляется проверка условия завершения времени функционирования ИТКС СН в заданном районе $t_{\text{функц.}}$. В случае завершения времени функционирования завершается функционирование ИТКС СН. В обратном случае переходят к блоку 16 рис. 4, в котором осуществляется функционирование ИТКС СН по назначению.

В блоке 17 рис. 4 моделируется изменение времени на единицу модельного времени Δt.

Далее (блоки 18 – 24, рис. 4), осуществляются процессы, функционирующие параллельно и независимо друг от друга в соответствующих подсистемах системы управления РЗ (рис. 2):

в блоке 18 рис. 4 осуществляется управление ИТКС СН на основе прогноза изменения РЗ, осуществляемого в центре управления РЗ ИТКС СН (рис. 2);

в блоке 19 рис. 4 осуществляется управление ИТКС СН на основе измерения состояния ИТКС СН по результатам мониторинга состояния ИТКС СН (рис. 2);

в блоке 20 рис. 4 осуществляется управление ИТКС СН на основе измерения условий оперативной обстановки, выражающееся в виде изменения плана ведения конфликта, поступающего от вышестоящей системы – системы управления (рис. 2);

в блоке 21 рис. 4 осуществляется мониторинг параметров элементов ИТКС СН, влияющих на показатели РЗ и характеризующих качество функционирования ИТКС СН по назначению;

в блоке 22 рис. 4 системой разведки защищающейся стороны осуществляется сбор и обновление данных о системе разведки нападающей стороны (рис. 2);

в блоке 23 рис. 4 осуществляется мониторинг значений параметров окружающей среды – сигнально-помеховой обстановки и климатических условий;

в блоке 24 рис. 4 осуществляется контроль наличия и состояния ресурсов по управлению РЗ элемента ИТКС СН.

Ниже рассматриваются алгоритмы осуществления действий, выполняемых в блоках 18 – 24, рис. 4.

На рис. 6 представлена блок-схема алгоритма, реализующего функции блока 18 рис. 4.

При передаче управления блоку 18 рис. 6 одновременно запускаются три параллельных процесса, направленных на вычисление бинарных переменных: Pr_R, характеризующей изменение информации о СР нападающей стороны (блоки 18.1 – 18.6, рис. 6), Pr_F, характеризующей изменение информации о значении характеристик о ИТКС СН (блоки 18.7 – 18.16, рис. 6), и Pr_S, характеризующей изменение информации о состоянии окружающей среды (блоки 18.17 – 18.21, рис. 6), определение выполнения условий (35). Значение переменных Pr_R, Pr_F, Pr_S равное 1 соответствует тому, что поступившая от соответствующих подсистем системы управления РЗ ИТКС СН текущая информация о значениях характеристик не соответствует заданным значениям характеристик СР нападающей стороны, ИТКС СН и окружающей среды, соответственно. Принятие переменными Pr_R, Pr_F, Pr_S значений равных 0 свидетельствует о том, что текущая информация, поступающая от соответствующих подсистем, соответствует имеющейся.

Вычисление значений переменной Pr_R осуществляется следующим образом:

в блоке 18.1 рис. 6 проводится считывание текущей информации о СР нападающей стороны ($I_{\text{СР тек.}}$) из памяти, в которую данная информация поступила от СР защищающейся стороны;

в блоке 18.2 рис. 6 проводится сравнение $I_{\text{СР тек.}}$ с информацией о СР нападающей стороны, имеющейся в центре управления РЗ ИТКС СН (рис. 2) $I_{\text{СРзад.}}$. В случае несовпадения поступившей текущей информации о СР нападающей стороны и имеющейся информации в центре управления РЗ ИТКС СН переходят к блоку 18.3 рис. 6. В противоположном случае переходят к блоку 18.6 рис. 6;

в блоке 18.3 рис. 6 проводится актуализация информации о СР нападающей стороны;

в блоке 18.4 рис. 6 актуализированная информация о СР запоминается в памяти центра управления РЗ ИТКС СН;

в блоке 18.5 рис. 6 бинарная переменная Pr_R устанавливается равной 1;

в блоке 18.6 рис. 6 бинарная переменная Pr_R устанавливается равной 0.

Вычисление значений переменной Pr_F осуществляется в блоках 18.7 – 18.16 рис. 6, аналогично вычислению Pr_R. Определение значения Pr_F осуществляется путем сравнения имеющейся в центре управления РЗ ИТКС СН информации о значениях характеристик ($i_{\text{х.зад.}jk}$, где j – номер элемента ИТКС СН, j=1, .., $N_{\text{ИТКС}}$; k – номер характеристики элемента ИТКС СН, k=1, .., $N_{\text{х.}j}$), влияющих на показатели РЗ элементов ИТКС СН, с текущими значениями данных характеристик ($i_{\text{х.тек.}jk}$), полученными от подсистемы мониторинга состояния ИТКС СН.

Вычисление значений переменной Pr_S осуществляется в блоках 18.17 – 18.22 рис. 6, аналогично вычислению Pr_R и Pr_F. Определение значения Pr_S осуществляется путем сравнения имеющейся в центре управления РЗ ИТКС СН информации о состоянии среды ($I_{S.\text{зад.}}$), с текущей информацией о состоянии среды ($I_{S.\text{тек.}}$), полученной от подсистемы мониторинга состояния среды.

В блоке 18.23 рис. 6 проверяется условие равенства 0 значений переменных Pr_R, Pr_F, Pr_S, определение выполнения условий (35). В случае невыполнения условия осуществляется переход к блоку 18.24 рис. 6, в противоположном случае осуществляется переход к блоку 18.37 рис. 6.

В блоке 18.24 рис. 6 задается цикл последовательного перебора всех элементов ИТКС СН.

В блоке 18.25 рис. 6 осуществляется оценка РЗ элемента ИТКС СН, для новых исходных данных, определенных в блоках 18.1 – 18.22 рис. 6, выражение (36).

Проверяют выполнение условия (37). Для чего, в блоке 18.26 рис. 6 проверяют условие равенства полученного значения оценки РЗ ($P_{\text{РЗ}j}$ ($t_{\text{мод.}}$+$t_{\text{сверт.}}$)) с оценкой, полученной ранее для предыдущих исходных данных $P_{\text{РЗ }i\text{ пред.}}$($t_{\text{мод.}}$+$t_{\text{сверт.}j}$). Сравнение проводится для текущего времени моделирования с учетом прибавления времени свертывания элемента ИТКС СН ($t_{\text{сверт.}j}$)

$$P_{\text{РЗ}j}(t+t_{\text{сверт.}j}) = P_{\text{РЗ }i\text{ пред.}}(t+t_{\text{сверт.}j}). \quad (45)$$

В случае невыполнения условия (45) переходят к блоку 18.27 рис. 6, в обратном случае переходят блоку 18.34 рис. 6.

В блоке 18.27 рис. 6 осуществляется проверка условия превышения полученного значения оценки РЗ ($P_{\text{РЗ}j}$ ($t_{\text{мод.}}$+$t_{\text{сверт.}}$)) над заданным предельно допустимого значения РЗ ($P_{\text{РЗ }j\text{ треб}}$), выражение (39):

$$P_{\text{РЗ}j}(t+t_{\text{сверт.}j}) \geq P_{\text{РЗ }j\text{ треб.}}. \quad (46)$$

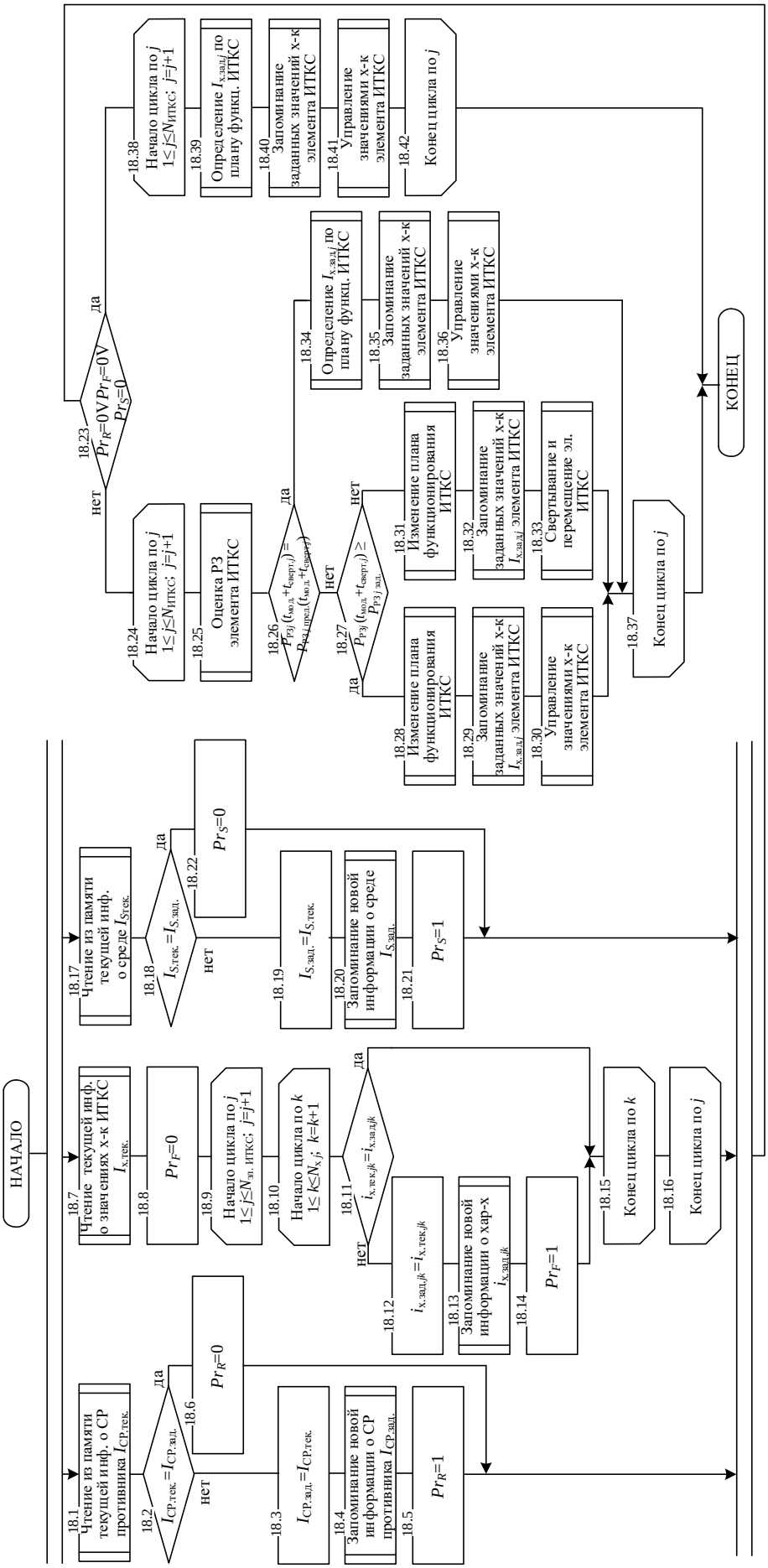

Рис. 6. Блок-схема алгоритма управление ИТКС СН
на основе прогноза изменения РЗ

В случае выполнения условия (46) переходят к блоку 18.28 рис. 6, в котором корректируют план функционирования ИТКС СН в направлении увеличения времени нахождения элемента ИТКС СН в заданном районе размещения, корректировка плана эквивалентна выполнению действий блоков 2-13 рис. 4. Далее переходят к блоку 18.29 рис. 6, в котором запоминают значения характеристик средств связи элемента ИТКС СН (информацию о заданных характеристиках элемента ИТКС СН $I_{\text{х.зад.}j}$), которые определены в новом плане функционирования ИТКС СН. В блоке 18.30 рис. 6 осуществляется управление характеристиками элемента ИТКС СН, в соответствии с запомненными значениями ($I_{\text{х.зад.}j}$). Далее переходят к блоку 18.37 рис. 6.

В случае невыполнения условия (46) переходят к блоку 18.31 рис. 6, в котором изменяется план функционирования ИТКС СН в направлении сокращения времени пребывания данного элемента ИТКС СН в заданном районе размещения. Далее переходят к блоку 18.32 рис. 6, в котором запоминают значения характеристик средств связи элемента ИТКС СН (информацию о заданных характеристиках элемента ИТКС СН $I_{\text{х.зад.}j}$). В блоке 18.33 рис. 6 осуществляется свертывание средств связи элемента ИТКС СН и перемещение элемента ИТКС СН в новый район размещения. Затем переходят к блоку 18.37 рис. 6.

Выполнение равенства (45) для отдельного элемента ИТКС СН эквивалентно, тому что для данного элемента ИТКС СН условия функционирования не изменились, поэтому в блоке 18.34 рис. 6 определяются характеристики, которые должны быть установлены для него по плану функционирования. Затем данные характеристики запоминаются (блок 18.35 рис. 6). В блоке 18.36 рис. 6 осуществляется управление характеристиками элемента ИТКС СН, в соответствии с запомненными значениями ($I_{\text{х.зад.}j}$). Затем переходят к блоку 18.37 рис. 6.

В блоке 18.37 рис. 6 выполняется проверка окончания цикла, заданного в блоке 18.24 рис. 6.

В блоке 18.38 рис. 6 задается цикл последовательного перебора всех элементов ИТКС СН.

Далее переходят к блоку 18.39 рис. 6, в котором определяют значения характеристик средств связи элемента ИТКС СН, которые должны быть установлены в соответствии с планом функционирования ИТКС СН. Затем в блоке 18.40 рис. 6 запоминают информацию об определенных значения характеристик средств связи элемента ИТКС СН ($I_{\text{х.зад.}j}$). В блоке 18.41 рис. 6 управляют значениями характеристик средств связи элемента ИТКС СН. В блоке 18.42 рис. 6 выполняется проверка окончания цикла, заданного в блоке 18.38 рис. 6. После завершения выполнения цикла, заданного в блоке 18.38 переходят к блоку 15 рис. 4.

При передаче управления блоку 19 рис. 4 запускается алгоритм, представленный на рис. 7.

В блоке 19.1 рис. 7 определяется перечень показателей качества функционирования ИТКС СН, состоящий из N позиций, выражение (40). Далее в соответствии с данным перечнем одновременно запускаются N параллельных алго-

ритмов, каждый из которых направлен на оценку качества функционирования ИТКС СН по заданному параметру.

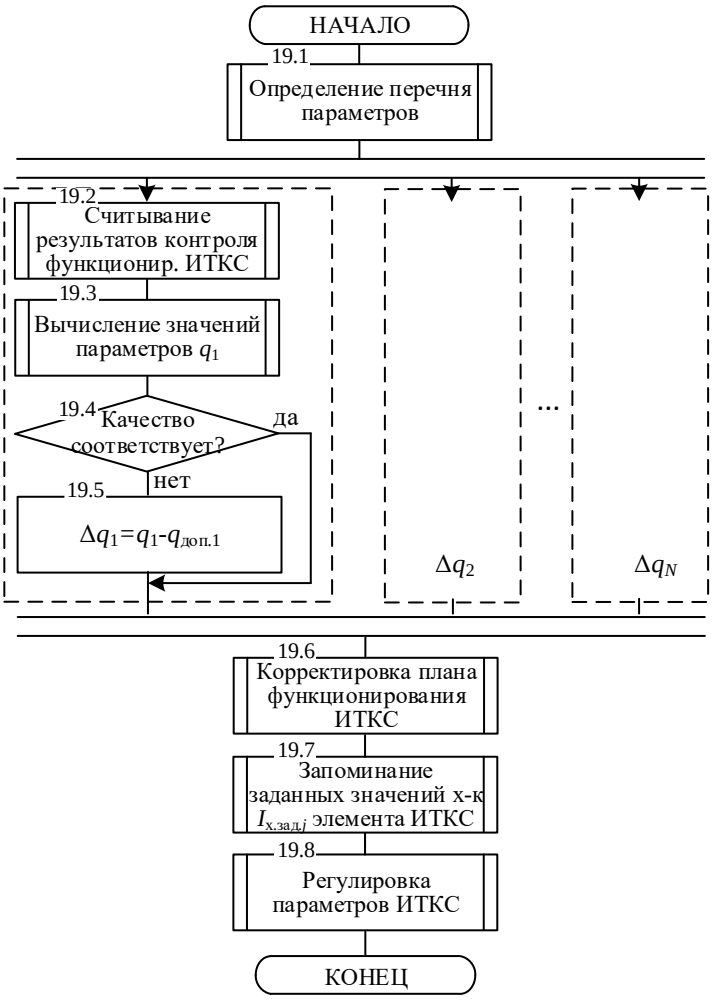

Рис. 7. Блок-схема алгоритма управления ИТКС СН на основе оценки параметров качества функционирования

Рис. 8. Блок-схема алгоритма управления ИТКС СН на основе изменения обстановки

В общем виде последовательность действий по оценке одного параметра качества функционирования ИТКС СН представлена блоками 19.2 – 19.4 рис. 7.

В блоке 19.2 рис. 7 осуществляется считывание из памяти значений результатов контроля функционирования ИТКС СН (множества O_i и Q_i, $\forall i, i = 1,..., N_{ИТКС}$), которые были получены в результате выполнения мониторинга функционирования ИТКС СН.

В блоке 19.3 рис. 7 осуществляется вычисление значения параметра качества функционирования элемента ИТКС СН q_1., выражение (41).

В блоке 19.4 рис. 7 осуществляется проверка условия соответствия определенного значения параметра качества функционирования заданным требованию (30). При выполнении условия (30) осуществляется переход к блоку 19.6 рис. 7, в обратном случае переходят к блоку 19.5 рис. 7.

В блоке блоку 19.5 рис. 7 вычисляется отклонение определенного значения параметра качества функционирования ИТКС СН от требуемого.

Аналогичным образом вычисляются разница между определенным и требуемым значениями параметра качества функционирования ИТКС СН.

В блоке 19.6 рис. 7 осуществляется корректировка плана функционирования ИТКС СН, корректировка плана эквивалентна выполнению действий блоков 2-13 рис. 4. Далее в блоке 19.7 рис. 7 запоминается информация о параметрах средств связи ИТКС СН, в блоке 19.8 рис. 7 осуществляется регулировка параметров ИТКС СН в целях удовлетворения требованиям качества функционирования ИТКС СН. Затем осуществляется переход к блоку 15 рис. 4.

При передаче управления блоку 20 рис. 4 запускается алгоритм, представленный на рис. 8.

В блоке 20.1 рис. 8 проводится определение изменений оперативных условий (ОУ). Данные изменения поступают в центр управления РЗ ИТКС СН от системы управления (рис. 1), они выражаются в виде целевой установки по обеспечению связью объектов системы управления.

В блоке 20.2 рис. 8 определяется соответствие изменений ОУ плану функционирования ИТКС СН. В случае соответствия ОУ плану переходят к блоку 15 рис. 4, в обратном случае переходят к блоку 20.3 рис. 8.

В блоке 20.3 рис. 8 корректируют план развертывания и функционирования ИТКС СН. Затем переходят к блоку 20.4 рис. 8, в котором настраивают ИТКС СН в соответствии с скорректированным планом функционирования ИТКС СН. Далее переходят к блоку 15 рис. 4.

При передаче управления блоку 21 рис. 4, в котором осуществляется мониторинг параметров элемента ИТКС СН (выражение (13)), влияющих на показатели РЗ и характеризующих качество функционирования ИТКС СН по назначению, выполняется последовательность действий, заданная алгоритмом (рис. 9).

В блоке 21.1 рис. 9 организуется цикл по перебору всех элементов ИТКС СН.

В блоке 21.2 рис. 9 организуется цикл по измерению значений параметров функционирования для выбранного в блоке 21.1 рис. 9 элемента ИТКС СН.

Для выбранного элемента ИТКС СН проводится измерение значений параметров соответствующими составляющими системы мониторинга, т.е. определяется значение параметра $o_{j,k}$ (блок 21.3 рис. 9).

В блоке 21.4 рис. 9 измеренные значения параметров элемента ИТКС СН записываются в память.

Далее в блоке 21.5 рис. 9 проверяется выполнение условия

$$o_{j,m_j} = o_{j,m_j\text{зад.}}, \forall j,\ j = 1,..., N_{ИТКС}, \tag{47}$$

где $o_{j,m_j\text{зад.}}$ – заданный по плану m_j-й параметр j-го элемента ИТКС СН.

В случае выполнение условия (47) переходят к блоку 21.7 рис. 9, в обратном случае переходят к блоку 21.6 рис. 9.

В блоке 21.6 рис. 9 сигнализируют в центр управления РЗ о необходимости изменения значения параметра $o_{j,k}$.

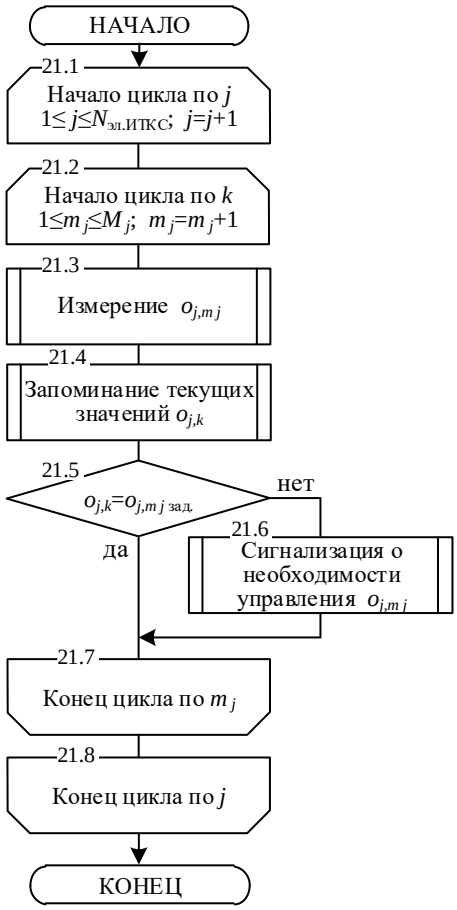

Рис. 9. Блок-схема алгоритма мониторинга параметров функционирования элемента ИТКС СН

Рис. 10. Блок-схема алгоритма обновления данных о СР нападающей стороны

В блоках 21.7 и 21.8 рис. 9 проверяют условия окончания циклов, заданных в блоках 21.2 и 21.1 рис. 9, соответственно.

После завершения выполнения циклов, заданных в блоках 21.1 и 21.2 рис. 9, переходят к блоку 15 рис. 4.

При передаче управления блоку 22 рис. 4 (выражение (15)), в котором осуществляется актуализация данных о СР нападающей стороны, выполняется последовательность действий, заданная алгоритмом (рис. 10).

В блоке 22.1 рис. 10 выполняется получение информации о СР нападающей стороны от СР защищающейся стороны $I_{СРполуч.}$.

В блоке 22.2 рис. 10 полученная информация о СР нападающей стороны сравнивается с имеющейся текущей информацией. В случае совпадения имеющейся и новой информации о СР нападающей стороны переходят к блоку 15 рис. 4, в обратном случае переходят к блоку 22.3 рис. 10.

В блоке 22.3 рис. 10 проводится оценка динамики изменения состава и функционирования СР противника.

В блоке 22.4 рис. 10 проводится запоминание полученной информации $I_{СРполуч.}$ о СР противника. Далее переходят к блоку 15 рис. 4.

При передаче управления блоку 23 рис. 4, в котором осуществляется мониторинг значений параметров окружающей среды – сигнально-помеховой об-

становки и климатических условий (выражение (12)), выполняется последовательность действий, заданная алгоритмом, представленным на рис. 11.

В блоке 23.1 рис. 11 осуществляется считывание текущей информации о состоянии среды (сигнально-помеховой обстановки и климатических условий), которая актуализируется соответствующими подсистемами системы мониторинга (рис. 1).

В блоке 23.2 рис. 11 проверяется выполнение условия

$$I_{S\text{тек.}}=I_S, \quad (48)$$

где $I_{S\text{тек.}}$ – информация о текущем состоянии множества $S_{\text{тек}}$; I_S – информация о состоянии множества S, имеющаяся в центре управления РЗ.

В случае выполнения условия (48) переходят к блоку 15 рис. 4, в обратном случае переходят к блоку 23.2 рис. 11, в котором запоминают новую информацию о состоянии среды.

При передаче управления блоку 24 рис. 4, в котором осуществляется мониторинг наличия и состояния ресурсов по управлению РЗ (выражение (14)), выполняется последовательность действий, заданная алгоритмом, представленным на рис. 12.

В блоке 24.1 рис. 12 осуществляется считывание текущей информации о наличии и состоянии ресурсов по управлению РЗ ($Z_{\text{тек.}}$), которая актуализируется соответствующими подсистемами системы мониторинга (рис. 1).

В блоке 24.2 рис. 12 осуществляется запоминание считанной информации о наличии и состоянии ресурсов.

В блоке 24.3 рис. 12 проверяется выполнение условия

$$z_{\text{тек.}i,j}\geq z_{\text{треб.}i,j} \mid \forall i,\ i=1,...,N_{ИТКС};\forall j,\ j=1,...,J_i \quad (49)$$

где $z_{\text{треб.}}$ – требующееся количество ресурсов по повышению РЗ, согласно установленных вышестоящей системой норм.

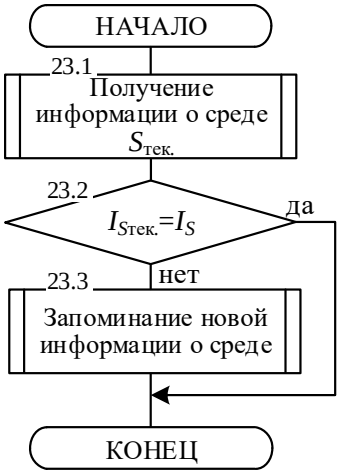

Рис. 11. Блок-схема алгоритма мониторинга состояния окружающей среды

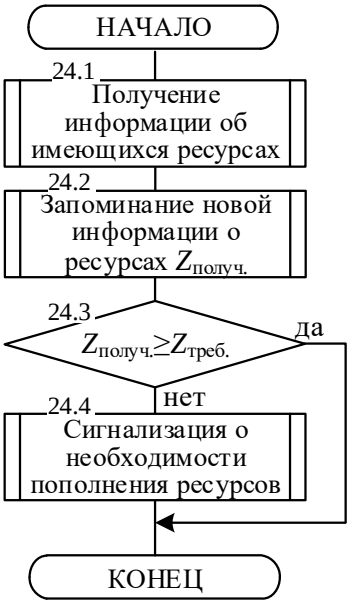

Рис. 12. Блок-схема алгоритма актуализации информации о состоянии ресурсов по управлению РЗ

В случае выполнения условия (49) переходят к блоку 15 рис. 4, в обратном случае переходят к блоку 24.4 рис. 12.

В блоке 24.4 рис. 12 сигнализируют системе управления (рис. 1) о необходимости пополнения ресурсов по управлению РЗ. Далее переходят к блоку 15 рис. 4.

Оценка адекватности метода защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта

Ключевые этапы алгоритма, реализующего метод защиты ИТКС СН (рис. 4), описываются блоками, позволяющими выработать решения по управлению параметрами элементов ИТКС СН на основе прогноза изменения РЗ в соответствии с условиями обстановки при условии обеспечения заданного качества функционирования ИТКС (1). Поэтому, адекватность метода можно оценить моделируя данные функции в процессе контрольного решения, которое представленного ниже. Учитывая это, за рамками контрольного решения (отнесено в ограничение) остались вопросы моделирования значений показателей РЗ и отдельных показателей качества функционирования ИТКС СН, ввиду их существенной зависимости от конкретных условий обстановки. В данном контрольном решении каждому конкретному действию множества W_i априорно ставится в соответствие изменение показателя РЗ и интегрального показателя качества функционирования $q_i=f(q_{i,g}),\ \forall i, i=1,...,N_{ИТКС}; \forall g, g=1,...,G_i$, на каждом конкретном элементе ИТКС СН, при чем, изменения $P_{РЗ}(t)$ и q_i в зависимости от применения любого действия по повышению РЗ имеют антагонистический характер. При этом, возможность выполнения каждого действия из множества W_i определяется наличием только одного ресурса из множества Z_i.

Исходные данные контрольного решения.

Имеется ИТКС СН, состоящая из пяти элементов $N_{ИТКС}=5$, расположенных на определенной местности (рис. 13). Все элементы ИТКС функционируют с интегральным качеством $q_i=0{,}95$.

К ИТКС применяются требования:

– по РЗ – время вскрытия элемента ИТКС СН должно быть не менее 4 ч с вероятностью 0,7;
– по качеству функционирования – интегральный коэффициент качества функционирования $q_i \geq 0{,}85$.

Разведку данной ИТКС СН ведет система разведки. При чем, на первоначальном этапе до начала управления имеется доступность демаскирующих признаков средств связи всех элементов ИТКС СН с вероятностью равной 1. Для вскрытия радиостанции системе разведки требуется перехватить не менее 10 сообщений. Элемент ИТКС считается вскрытым системой разведки в случае вскрытия всех средств связи, входящих в элемент.

Каждый элемент ИТКС СН характеризуется набором средств связи и параметрами их работы (таблица 2).

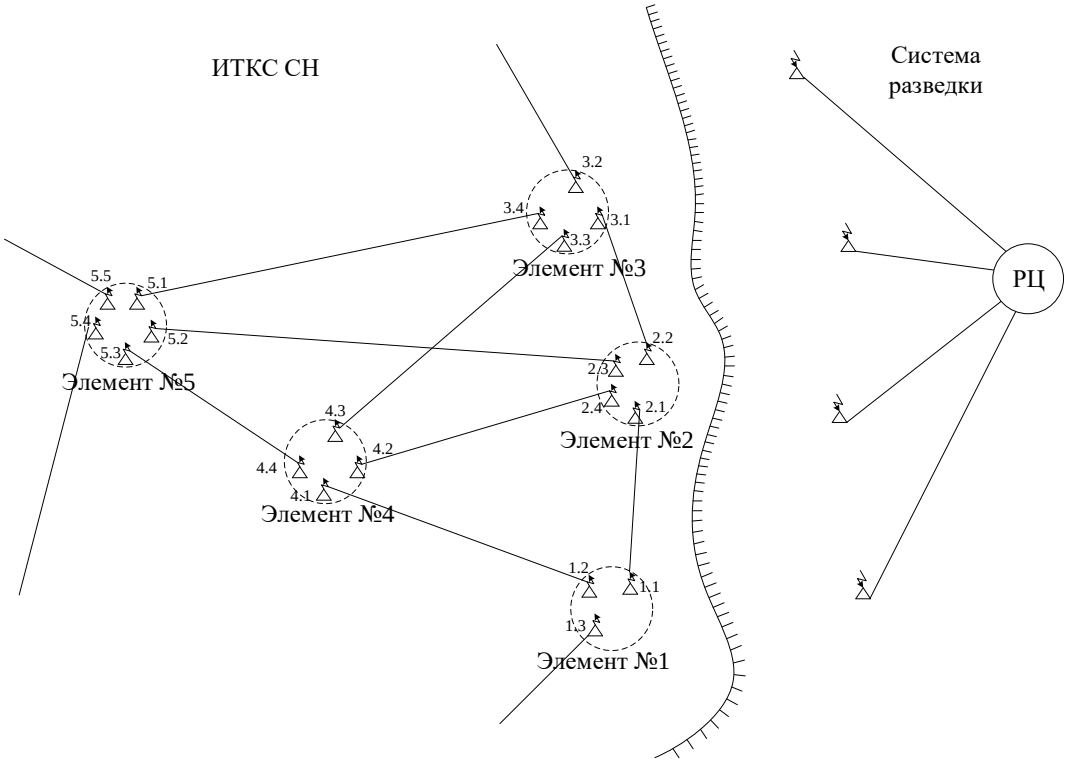

Рис. 13. Иллюстрация к контрольному решению
(РЦ – разведывательный центр)

Таблица 2 – Состав элементов ИТКС СН

№ п/п	№ элемента ИТКС	№ средства связи в элементе ИТКС	Интенсивность работы (μ), сообщ./час
1	1	1.1	3
2		1.2	5
3		1.3	3
4	2	2.1	3
5		2.2	3,5
6		2.3	3,2
7		2.4	6
8	3	3.1	3,5
9		3.2	3
10		3.3	4
11		3.4	2
12	4	4.1	5
13		4.2	6
14		4.3	4
15		4.4	10
16	5	5.1	2
17		5.2	3,2
18		5.3	10
19		5.4	8
20		5.5	15

Взаимосвязи элементов ИТКС СН (рис. 13) характеризуются соответствующими интенсивностями обмена информацией (таблица 3). Связность гра-

ничных элементов ИТКС СН с внешними ИТКС, характеризуется интенсивностью работы граничного средства связи.

Таблица 3 – Интенсивности обмена сообщениями между станциями связи ИТКС

№ СС	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1				3																
2																				
3			3																	
4	3																			
5								3,5												
6																				
7																				
8					3,5															
9									3											
10														4						
11																2				
12		5																		
13							6													
14										4										
15																	10			
16											2									
17						3.2														
18															10					
19																			8	
20																				15

Наличие доступных ресурсов по управлению РЗ на каждом элементе ИТКС, характеризуется соответствующим вектором z_i, где i=1,..,$N_{ИТКС}$, принадлежащим множеству Z. Элементами вектора являются признаки доступности того или иного ресурса, $z_{i,j}$ =1 при наличии j-го данного ресурса в i-м элементе ИТКС СН, и $z_{i,j}$=0 в случае его недоступности. В модели максимальный номер ресурса равен 10, т.е. j=1, ... ,10 (таблица 4).

Каждая реализация действия из множества W по использованию ресурсов множества Z, характеризуется материальными и временными затратами. Для контрольного примера затраты по реализации действий по повышению РЗ для всех элементов являются идентичными (таблица 5).

Таблица 4 – Доступность ресурсов управления РЗ в элементах ИТКС

Z \ j	1	2	3	4	5	6	7	8	9	10
z_1	1	0	0	1	1	0	1	1	0	1
z_2	1	1	0	1	0	1	1	1	0	1
z_3	0	1	1	1	0	0	1	1	0	1
z_4	1	1	0	1	0	0	1	1	1	1
z_5	1	1	1	1	1	1	1	1	1	1

Таблица 5 – Временные и материальные затраты по реализации действий повышения РЗ

Действие	*j* / Затраты	Номер ресурса									
		1	2	3	4	5	6	7	8	9	10
$W(z_i)$	$t_{реализ.i,j}$, час.	0,1	0,13	0,15	0,4	0,5	0,2	0,3	0,17	0,05	0,7
	$C_{реализ.i,j}$, у.е.	0,3	0,2	0,9	0,2	0,17	0,19	0,5	0,15	0,9	0,3

В соответствии с указанными ранее ограничениями контрольного решения эффект от действий по повышению РЗ для каждого элемента ИТКС СН определяется как снижение вероятности доступности элемента ИТКС средствам разведки в совокупности со снижением качества функционирования элемента ИТКС на величины, представленные в таблице 6.

Таблица 6 – Временные и материальные затраты по реализации действий повышения РЗ

Элемент ИТКС	*j* / Затраты	Номер действия из множества *W*									
		1	2	3	4	5	6	7	8	9	10
1	$\Delta P_{1,j}$	0,05	0,02	0,03	0,04	0,025	0,1	0,015	0,06	0,03	0,025
	$\Delta Q_{1,j}$	0,03	0,04	0,06	0,07	0,05	0,03	0,05	0,04	0,04	0,02
2	$\Delta P_{2,j}$	0,04	0,2	0,02	0,04	0,05	0,05	0,025	0,01	0,035	0,015
	$\Delta Q_{2,j}$	0,02	0,05	0,05	0,04	0,05	0,04	0,03	0,05	0,06	0,02
3	$\Delta P_{3,j}$	0,035	0,027	0,02	0,055	0,032	0,065	0,022	0,017	0,032	0,016
	$\Delta Q_{3,j}$	0,02	0,05	0,05	0,06	0,051	0,05	0,027	0,045	0,05	0,021
4	$\Delta P_{4,j}$	0,03	0,025	0,05	0,25	0,033	0,06	0,024	0,15	0,029	0,17
	$\Delta Q_{4,j}$	0,021	0,045	0,06	0,037	0,06	0,037	0,05	0,04	0,05	0,023
5	$\Delta P_{5,j}$	0,05	0,1	0,05	0,06	0,093	0,02	0.26	0,02	0,031	0,017
	$\Delta Q_{5,j}$	0,01	0,02	0,03	0,02	0.04	0.025	0.34	0,06	0.05	0,025

Результаты контрольного решения.

Результаты моделирования выполнения основных функций метода, реализованного алгоритмом (рис. 4), по приведенным выше исходным данным представлены ниже.

При предположении того, что все проявления демаскирующих признаков при их доступности попадают в систему разведки на обработку полученные зависимости вероятности вскрытия элементов ИТКС СН от времени представлены на рис. 14.

Анализ зависимостей, представленных на рис. 14 и результаты вычислений по выражению (2), представленные в таблице 7, свидетельствуют о том, что требования по РЗ выполняются только для элемента ИТКС с номером №3.

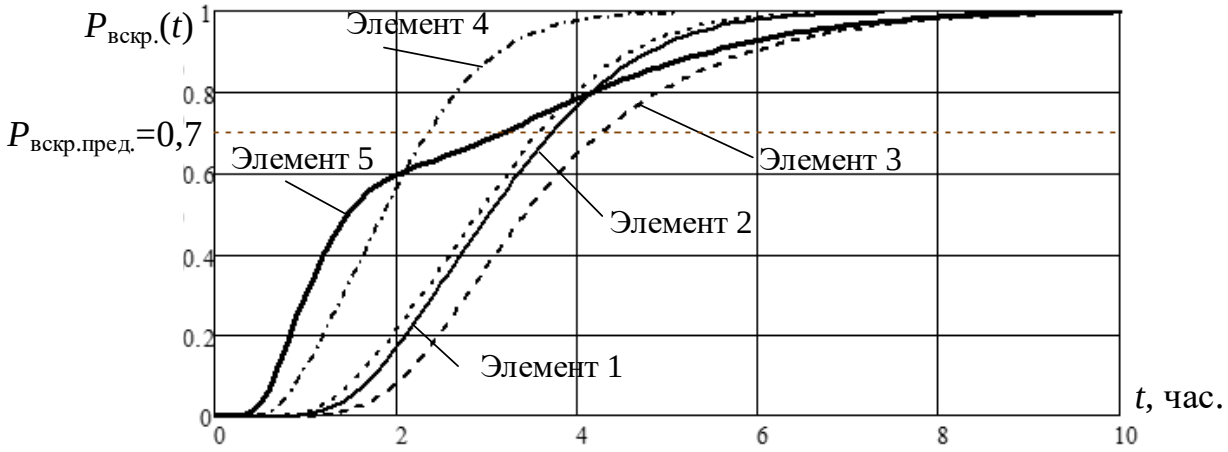

Рис. 14. Зависимости вероятности вскрытия элементов ИТКС СН

Таблица 7 – Время вскрытия элементов ИТКС

Номер элемента ИТКС	1	2	3	4	5
$t_{вскр.i}$	3 ч 43 мин	3 ч 35 мин	4 ч 16 мин	2 ч 21 мин	3 ч 11 мин

Далее проводится определение необходимого набора действий по повышению РЗ на элементах с номерами 1, 2, 4, 5. Затем проводится поиск оптимального набора действий по повышению РЗ в соответствии с алгоритмом, представленным на рис. 5, и выражениями (5) и (7). Результаты данных вычислений на примере элемента №5 представлены на рис. 15.

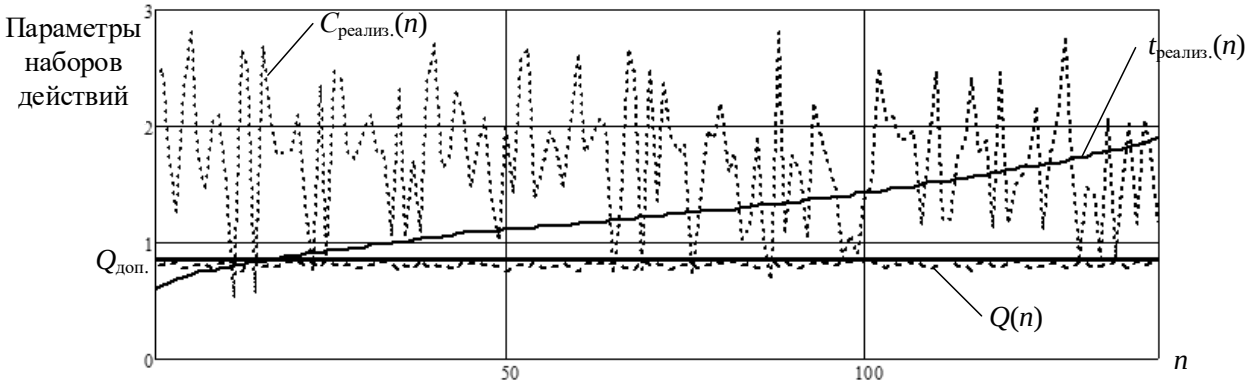

Рис. 15. Зависимости времени $t_{реализ.}(n)$, стоимости $C_{реализ.}(n)$, интегрального коэффициента эффективности функционирования $Q(n)$ для элемента №5 от номера набора действий по повышению РЗ (n – номер набора действий)

Анализ зависимостей, представленных на рис. 15, позволил определить оптимальный набор действий из 141 варианта доступных по критерию $t_{реализ.}(n)\rightarrow\min|\ Q\geq Q$доп. Оптимальный вариант действий по повышению РЗ является вариант при n=15 с пятью различными доступными действиями, при котором $Pr_{действ.5\ 0,1,2,7,8}$=1.

В результате применения варианта набора действий по повышению РЗ время вскрытия элемента №5 ИТКС СН увеличилось с 3 ч 11 мин до 4 ч 9 мин,

что свидетельствует о выполнении требований по РЗ, при этом, интегральный коэффициент качества функционирования по назначению снизился до допустимых значений с 0,95 до 0,865.

Аналогичные результаты получены для остальных элементов исследуемой ИТКС СН, что свидетельствует об адекватности предложенного метода управления защитой ИТКС СН.

За рамками данного контрольного решения остались вопросы управления изменением структурой ИТКС СН. Однако, следует отметить, что при управлении ИТКС СН в условиях конфликта требуется постоянно изменять ее состояние, заключающееся в смене режимов работы средств связи, входящих в состав элементов ИТКС СН, а также смене мест размещения элементов ИТКС СН. При реализации данных действий зависимости значений показателей РЗ от радиоразведки будут иметь вид аналогичный представленному в работе [4]. Для других видов технической разведки требуется проведение отдельных исследований зависимостей показателей РЗ, так как, например, при перемещениях элементов ИТКС СН они становятся более доступными для видовых разведок, чем при расположении в районе с применением инженерных средств маскировки.

Выводы

Разработанный метод защиты ИТКС СН в условиях информационного конфликта, позволяет усовершенствовать процесс управления ИТКС по критерию выполнения требований по оперативности и обоснованности реагирования на изменение обстановки при управлении РЗ ее элементов с учетом основных факторов. Обоснован перечень факторов, оказывающих существенное влияние на показатели РЗ при соблюдении требований к качеству функционирования ИТКС СН по назначению. При формировании управленческих решений элементам ИТКС СН учитывается наличие ограниченных ресурсов на каждом элементе, а также результативность их использования при повышении РЗ.

Новизной представленного решения является расширение количества параметров, описывающего исходные данные, учет динамики и прогнозирования его изменения при выработке управленческих решений элементами ИТКС СН в условиях конфликта. В результате чего повышается обоснованность управления, полное и эффективное использование боевых возможностей ИТКС СН.

Разработанный метод является дальнейшим развитием теории управления ИТКС СН и в отличие от известных обладает расширенными функциональными возможностями по решению различных задач при анализе и синтезе защищенных систем СН функционирующих в условиях информационного конфликта. Он может быть использован при создании информационно-аналитических комплексов в системах поддержки принятия решений по защите ИТКС СН, в том числе и с использованием методов искусственного интеллекта, а также при обосновании требований к ИТКС СН, их элементам, средствам и комплексам связи, входящим в состав элементов ИТКС СН.

Дальнейшее развитие представленного метода планируется в направлении добавления методов интеллектуализации при выработке управленческих

решений, а также совершенствовании моделей, направленных на оценку РЗ и качества функционирования ИТСК СН.

Литература

1. Макарчук И. Л., Троценко К. А. Характер операций современных армий – назревшие изменения // Военная мысль. 2022. № 12. С. 12–26.

2. Романчук А. В., Шигин А. В. Перспективы повышения эффективности армейских оборонительных операций // Военная мысль. 2023. № 4. С. 23–33.

3. Круглов В. В., Воскресенский В. Г., Мурсаметов В. Я. Тенденции развития вооруженной борьбы в XXI веке и их влияние на военное искусство зарубежных стран // Военная мысль. 2023. № 4. С. 124–133.

4. Стародубцев Ю. И, Липатников В. А., Парфиров В. А. Проблема повышения разведывательной защищенности элементов военной системы связи // Военная мысль. 2023. № 7. С. 88–99.

5. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 182 с.

6. Куприянов А. И., Петренко П. Б. Теоретические основы радиоэлектронной разведки: учеб. пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. 388 с.

7. Меньшаков Ю. К. Теоретические основы технических разведок. М.: ИПЦ «Маска», 2017. 640 с.

8. Михайлов Р. Л. Радиоэлектронная борьба в Вооруженных силах США: военно-теоретический труд. СПб.: Наукоемкие технологии, 2018. 131 с.

9. Костарев С. В., Воробьев И. Г. Современные подходы к обеспечению разведывательной защищенности и живучести системы связи объединения в операциях (боевых действиях) // Военная мысль. 2019. № 11. С. 58–68.

10. Иванов В. Г., Гудков М. А., Лукьянчик В. Н. Единое информационное пространство ВС РФ – основа информационного обеспечения войск в международных вооруженных конфликтах // Военная мысль. 2023. № 5. С. 85–95.

11. Военный энциклопедический словарь. М.: Воениздат, 2007. 832 с.

12. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. СПб.: Наукоемкие технологии, 2020. 337 с.

13. Липатников В. А., Соломатин А. И., Терентьев А. В. Радиопеленгация. Теория и практика. СПб.: ВАС, 2006. 356 с.

14. Липатников В. А., Царик О. В. Методы радиоконтроля. Теория и практика: Монография. СПб.: ГНИИ «НАЦРАЗВИТИЕ», 2018. 608 с.

15. Джамалидинова М. Е., Пищин О. Н. Нечеткая продукционная модель управления уровнем поля в системах подвижной связи // Приоритетные научные направления: от теории к практике. 2016. № 34-1. С. 171–176.

16. Штрагер Е. А. Физические основы стелс-технологий. СПб.: ООО «Издательство ВВМ», 2013. 279 с.

17. Липатников В. А., Парфиров В. А. Метод маскировки районов расположения объектов критически важной инфраструктуры от

радиолокационных средств наблюдения // Труды Военно-космической академии имени А.Ф. Можайского. 2023. № 686. С. 68–77.

18. Козлов С. В. Методы и средства радиоэлектронной защиты: учебное пособие. Минск: Белорусский государственный университет информатики и радиоэлектроники. 2019. 188 с.

19. Меньшаков Ю. К. Основы защиты от технических разведок: учеб. пособие / Под общ. ред. М. П. Сычева. М.: Изд-во МГТУ им. Баумана, 2011. 478 с.

20. Гречишников Е. В., Стародубцев Ю. И., Белов А. С., Стукалов И. В., Васюков Д. Ю., Иванов И. В. Способ (варианты) управления демаскирующими признаками системы связи // Патент RU № 2450337 C1, опубл. 10.05.2012, бюл. № 13.

21. Гречишников Е. В., Добрышин М. М., Чукляев И. И., Горелик С. П. Способ динамического управления параметрами сети связи в признаковом пространстве // Патент RU № 2597457 C1, опубл. 10.09.2016 г., бюл. № 25.

22. Алешин О. В., Сызранцев А. Г., Федулов А. В. Технологические основы построения автоматических систем управления связью высокодинамичных систем управления специального назначения // I-methods. 2019. Т. 11. № 1. С. 52–65.

23. Макаренко С. И. Справочник научных терминов и обозначений. СПб.: Наукоемкие технологии, 2019. 254 с.

24. Боговик А. В., Игнатов В. В. Теория управления в системах военного назначения. Учебник. СПб.: ВАС, 2008. 460 с.

25. Яресь О. Б., Паньшин И. В. Методы принятия управленческих решений: учеб. пособие. Владимир: Изд-во Владим. гос. ун-та имени Александра Григорьевича и Николая Григорьевича Столетовых, 2011. 66 с.

26. Стародубцев Ю. И., Иванов С. А., Вершенник Е. В., Вершенник А. В., Закалкин П. В., Константинов С. А., Спицын О. Л. Способ управления состоянием сложного объекта // Патент на изобретение RU 2748778 C1, опубл. 31.05.2021, бюл. № 16.

27. Стародубцев Ю. И., Остроумов О. А., Вершенник Е. В., Лепешкин О. М., Синюк А. Д., Перов Р. А., Карпов М. А., Митрофанова Т. Ю., Черных И. С., Лапин С. П. Способ обеспечения устойчивого функционирования сложного программно-аппаратного объекта сложной функционально-динамической структуры // Патент на изобретение RU 2787274 C1, опубл. 09.01.2023, бюл. № 1.

28. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4 (89). С. 67–76. doi: 10.15217/issnl684-8853.2017.4.67.

29. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства: Научная монография / под общ. ред. В. А. Липатникова. СПб.: ВАС, 2020. 716 с.

30. Алашев В. В., Вершенник А. В., Вершенник Е. В., Латушко Н. А., Стародубцев Ю. И., Чеснаков М. А. Способ моделирования конфликтных ситуаций // Патент на изобретение RU 2662646 C1, опубл. 26.07.2018, бюл. № 21.

31. Шевчеко А. А. Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции. СПб.: ВАС, 2020. С. 237–241.

32. Алиев Т. И. Основы моделирования дискретных систем. СПб: СПбГУ ИТМО, 2009. 363 с.

33. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. СПб.: ВАС, 2021. 192 с.

34. Саати Т. Л. Математические модели конфликтных ситуаций / Пер. с англ. Под ред. И. А. Ушакова. М.: Советское радио, 1977. 304 с.

35. Новиков Д. А. Теория управления организационными системами. М.: МПСИ, 2005. 584 с.

36. Липатников В. А., Парфиров В. А. Пути повышения адекватности моделирования разведывательной защищенности объектов Вооруженных сил // Военная безопасность России: взгляд в будущее: Материалы 8-й Международной межведомственной научно-практической конференции. М.: Изд. МГТУ им. Н. Э. Баумана, 2023. С. 343–349.

37. Акиншин Р. Н., Анищенко А. В., Ашурбейли И. Р. и др. Модели технических разведок и угроз безопасности информации: Монография / Ред. Е. М. Сухарев. М.: Радиотехника, 2003. 142 с.

38. Липатников В. А., Парфиров В. А. Вероятностно-временные показатели процесса выявления сетей радиосвязи // Инновационные технологии и технические средства специального назначения: Труды XV научно-практической конференции. СПб.: БГТУ «Военмех», 2023. С. 172–175.

39. Барабаш Ю. Л. Коллективные статистические решения при распознавании. М.: Радио и связь, 1983. 224 с.

40. Мазуров В. Д. Математические методы распознавания образов. Учебное пособие. Екатеринбург: Уральский государственный университет им. А.М. Горького, 2010. 101 с.

41. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся втузов. М.: Наука, 1986. 544 с.

42. Кушнир Ф. В. Электрорадио измерения: Учебное пособие для вузов. Л.: Энергоатомиздат,1983. 320 с.

43. Липатников В. А., Парфиров В. А., Петренко М. И. Общий алгоритм динамического управления устойчивым функционированием сети связи специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция. СПб.: СПбГУТ, 2023. С. 814–819.

44. Воронов Е. М., Карпунин А. А. Алгоритмы иерархической оптимизации в двухуровневой многоканальной задаче "управление-

регулирование" // Вестник Российского университета дружбы народов. Серия: Инженерные исследования. 2009. № 4. С. 55–67.

45. Липатников В. А., Парфиров В. А. Модель процесса наблюдения за множеством источников информации в стохастических условиях // Информация и космос. 2022. № 1. С. 35–44.

46. Парфиров В. А. Математическая модель динамики перемещений локально распределенного группового объекта // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2022. № 9–10 (171–172). С. 50–57.

47. Липатников В. А., Сахаров Д. В., Парфиров В. А., Петренко М. И. Моделирование функционирования распределенного объекта радиоконтроля // Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. СПб.: Региональная общественная организация «Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления», 2022. С. 599–604.

48. Липатников В. А., Парфиров В. А. Способ моделирования местонахождения объектов группы с учетом динамики перемещений // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции. СПб.: ВАС, 2022. С. 253–258.

49. Липатников В. А., Парфиров В. А. Вероятностные характеристики процесса определения местоположения объектов радиоконтроля с учетом стохастичности параметров излучений и помех. // Актуальные проблемы защиты и безопасности: Труды XXV Всероссийской научно-практической конференции. СПб: РАРАН, 2022. С. 299–304.

50. Липатников В. А., Парфиров В. А. Вероятностно-временные характеристики процесса измерения координат робототехнических комплексов военного назначения по излучаемым радиосигналам // Перспективные системы и задачи управления: сборник трудов XVII Всероссийской конференции. Таганрог, 2022. С. 214–220.

51. Липатников В. А., Парфиров В. А., Мелехов К. В. Модель определения вероятностно-временных характеристик обнаружения объектов при неоднократном обследовании местности // Актуальные проблемы защиты и безопасности: Труды XXVI Всероссийской научно-практической конференции. СПб: Типография Любавич, 2023. С. 563–568.

52. Сызранцев Г. В. Теоретические и научно-методические основы обеспечения построения сложных организационно-технических систем военной связи в локальных войнах и вооруженных конфликтах: Монография / Под ред. профессора А. Г. Ермишяна. СПб.: ВАС, 2007. 180 с.

53. Гурин Л. С., Дымарский Я. С., Меркулов А. Д. Задачи и методы оптимального распределения ресурсов. М.: Советское радио, 1968. 463 с.

54. Берзин Е. А. Оптимальное распределение ресурсов и теория игр. М.: Радио и связь, 1983. 216 с.

55. Берзин Е. А. Оптимальное распределение ресурсов и элементы синтеза систем. М.: Советское радио, 1974. 304 с.

56. Михайлов Р. Л., Поляков С. Л. Модель оптимального распределения ресурсов и исследование стратегий информационного конфликта // Системы управления связи и безопасности. 2018. № 4. С. 323–344.

57. Моисеев Н. Н., Иванилов Ю. П., Столярова Е. М. Методы оптимизации. М.: Наука, 1978. 352 с.

58. Бусов В. И. Управленческие решения: учебник для академического бакалавриата. М.: Издательство Юрайт, 2019. 254 с.

59. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях: Ч. 1. Методологические основы построение организационно-технических систем военной связи. СПб.: ВАС, 2005. 740 с.

60. Дмитрюк А. М. Касанин С. Н., Градусов Р. А., Антоненко И. В. Основы организации связи: учебно-методическое пособие. Минск: БГУИР, 2012. 150 с.

61. Алтухов П. К., Афонский И. А., Рыболовский И. В., Татарченко А. Е. Основы теории управления войсками / под ред. П. К. Алтухова. М.: Воениздат, 1984. 221 с.

62. Липатников В. А., Сахаров Д. В., Парфиров В. А., Петренко М. И. Имитационная модель распределенного объекта радиоконтроля, отражающая динамику перемещений и смену режимов работы радиоэлектронных средств // Региональная информатика (РИ-2022): Юбилейная XVIII Санкт-Петербургская международная конференция. СПб.: Региональная общественная организация «Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления», 2022. С. 556–558.

References

1. Makarchuk I. L., Trotsenko K. A. The nature of operations of modern armies - overdue changes. *Military thought*, 2022, no. 12, pp. 12–26 (in Russian).

2. Romanchuk A. V., Shigin A. V. Prospects for improving the effectiveness of army defensive operations. *Military thought*, 2023, no. 4, pp. 23–33 (in Russian).

3. Kruglov V. V., Voskresensky V. G., Mursametov V. Ya. Trends in the development of armed struggle in the XXI century and their impact on the military art of foreign countries. *Military thought*, 2023, no. 4, pp. 124–133 (in Russian).

4. Starodubtsev Yu. I., Lipatnikov V. A., Parfirov V. A. The problem of increasing the intelligence security of elements of the military communications system. *Military thought*, 2023, no. 7, pp. 88–99 (in Russian).

5. Bogovik A. V., Ignatov V. V. *Jeffektivnost' sistem voennoj svjazi i metody ee ocenki* [Efficiency of military communication systems and methods of its evaluation]. Saint-Petersburg, Military Academy of Communications Publ., 2006. 182 p. (in Russian).

6. Kupriyanov A. I., Petrenko P. B. *Teoreticheskie osnovy radiojelektronnoj razvedki* [Theoretical foundations of electronic intelligence]. Moscow, Publishing

House of Bauman Moscow State Technical University Publ., 2009. 388 p. (in Russian).

7. Menshakov Yu. K. *Teoreticheskie osnovy tehnicheskih razvedok* [Theoretical foundations of technical intelligence]. Moscow, Izdatel'sko-poligraficheskij centr «Maska» Publ., 2017. 640 p. (in Russian).

8. Mikhailov R. L. *Radiojelektronnaja bor'ba v Vooruzhennyh silah SShA: voenno-teoreticheskij trud* [Electronic warfare in the US Armed Forces: military-theoretical work]. Saint-Petersburg, Naukoemkie tehnologii Publ., 2018. 131 p. (in Russian).

9. Kostarev S. V., Vorobyev I. G. Modern approaches to ensuring intelligence security and survivability of the association's communication system in operations (combat operations). *Military Thought*, 2019, no. 11, pp. 58–68 (in Russian).

10. Ivanov V. G., Gudkov M. A., Lukyanchik V. N. Unified information space of the Armed Forces of the Russian Federation – the basis of information support of troops in international armed conflicts. *Military Thought*, 2023, no. 5, pp. 85–95 (in Russian).

11. *Voennyj jenciklopedicheskij slovar'* [Military encyclopedic dictionary]. Moscow, Voenizdat Publ., 2007. 832 p. (in Russian).

12. Makarenko S. I. *Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. Monografija* [Models of the communication system in conditions of deliberate destabilizing influences and intelligence. Monograph]. Saint-Petersburg, Naukoemkie tehnologii Publ., 2020. 337 p. (in Russian).

13. Lipatnikov V. A., Solomatin A. I., Terentyev A. V. *Radiopelengacija. Teorija i praktika* [Radio direction finding. Theory and practice]. Saint-Petersburg, Military Academy of Communications Publ., 2006. 356 p. (in Russian).

14. Lipatnikov V. A., Tsarik O. V. *Metody radiokontrolja. Teorija i praktika: Monografija* [Methods of radio control. Theory and practice: Monograph]. Saint-Petersburg, Gumanitarnyj nacional'nyj issledovatel'skij institut «Nacrazvitie» Publ., 2018. 608 p. (in Russian).

15. Jamalidinova M. E., Pishchin O. N. Fuzzy production model of field level control in mobile communication systems. *Priority scientific directions: from theory to practice*, 2016, no. 34-1, pp. 171–176 (in Russian).

16. Shtrager E. A. *Fizicheskie osnovy stels-tehnologij* [Physical foundations of stealth technologies]. Saint-Petersburg, Obshhestvo s ogranichennoj otvetstvennost'ju "OOO «Izdatel'stvo VVM» Publ., 2013. 279 p. (in Russian).

17. Lipatnikov V. A., Parfirov V. A. Method of masking areas of location of critical infrastructure objects from radar surveillance means. *Proceedings of the Mozhaisky Military Space Academy*, 2023, no. 686, pp. 68–77 (in Russian).

18. Kozlov S. V. *Metody i sredstva radiojelektronnoj zashhity* [Methods and means of electronic protection]. Minsk, Belarusian State University of Informatics and Radioelectronics Publ., 2019. 188 p. (in Russian).

19. Menshakov Yu. K. *Osnovy zashhity ot tehnicheskih razvedok* [Fundamentals of protection from technical intelligence]. Under the general

editorship of M. P. Sychev. Moscow, Publishing house of Bauman Moscow State Technical University Publ., 2011. 478 p. (in Russian).

20. Grechishnikov E. V., Starodubtsev Yu. I., Belov A. S. Stukalov I. V., Vasjukov D. Ju., Ivanov I. V. *Sposob (varianty) upravlenija demaskirujushhimi priznakami sistemy svjazi* [Method (options) for controlling the unmasking features of a communication system]. Patent Russia, no. RU 2450337 C1. 2012. (in Russian).

21. Grechishnikov E. V., Dobryshin M. M., Chuklyaev I. I., Gorelik S. P. *Sposob dinamicheskogo upravlenija parametrami seti svjazi v priznakovom prostranstve* [Method of dynamic control of parameters of a communication network in a feature space]. Patent Russia, no. RU 2597457 C1. 2016. (in Russian).

22. Aleshin O. V., Syzrantsev A. G., Fedulov A. V. Technological bases for constructing automatic communication control systems of highly dynamic special purpose control systems. *I-methods*, 2019, vol. 11, no. 1, pp. 52–65 (in Russian).

23. Makarenko S. I. *Spravochnik nauchnyh terminov i oboznachenij* [Handbook of Scientific Terms and Designations]. Saint-Petersburg, Naukoemkie tehnologii Publ., 2019. 254 p. (in Russian).

24. Bogovik A. V., Ignatov V. V. *Teorija upravlenija v sistemah voennogo naznachenija* [Theory of control in military systems]. Saint-Petersburg, Military Academy of Communications Publ., 2008. 460 p. (in Russian).

25. Yares O. B., Panshin I. V. *Metody prinjatija upravlencheskih reshenij* [Methods of managerial decision-making]. Vladimir: Publishing House of the Vladimir State University named after Alexander Grigoryevich and Nikolai Grigoryevich Stoletov Publ., 2011. 66 p. (in Russian).

26. Starodubtsev Yu. I., Ivanov S. A., Vershennik E. V. Vershennik A. V., Zakalkin P. V., Konstantinov S. A., Spicyn O. L. *Sposob upravlenija sostojaniem slozhnogo ob#ekta* [A way to manage the state of a complex object]. Patent Russia, no. RU 2748778 C1. 2021. (in Russian).

27. Starodubtsev Yu. I., Ostroumov O. A., Vershennik E. V., Lepeshkin O. M., Sinjuk A. D., Perov R. A., Karpov M. A., Mitrofanova T. Ju., Chernyh I. S., Lapin S. P. *Sposob obespechenija ustojchivogo funkcionirovanija slozhnogo programmno-apparatnogo ob#ekta slozhnoj funkcional'no-dinamicheskoj struktury* [A method for ensuring the stable functioning of a complex hardware and software object of a complex functional and dynamic structure]. Patent Russia, no. RU 2787274 C1. 2023. (in Russian).

28. Lipatnikov V. A., Shevchenko A. A., Yatskin A. D., Semenova E. G. Information security management of an integrated structure organization based on a dedicated server with container virtualization. *Informatsionno-upravliaiushchie sistemy*, 2017, vol. 89, no. 4, pp. 67–76 (in Russian).

29. Kostarev S. V., Karganov V. V., Lipatnikov V. A. *Tehnologii zashhity informacii v uslovijah kiberneticheskogo protivoborstva: Nauchnaja monografija* [Information security technologies in the conditions of cybernetic confrontation: Scientific monograph]. Under the general editorship of V. A. Lipatnikov. Saint-Petersburg, Military Academy of Communications Publ., 2020. 716 p. (in Russian).

30. Alashev V. V., Vershennik A. V., Vershennik E. V. Latushko N. A., Starodubcev Ju. I., Chesnakov M. A. *Sposob modelirovanija konfliktnyh situacij*

[Method of modeling conflict situations]. Patent Russia, no. RU 2662646 C1. 2018. (in Russian).

31. Shevcheko A. A. *Matematicheskaja model' informacionnogo protivoborstva dvuh sistem v informacionno-telekommunikacionnom prostranstve. Innovacionnaja dejatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii* [Mathematical model of information confrontation between two systems in the information and telecommunications space. Innovative activity in the Armed Forces of the Russian Federation: Proceedings of the All-Army Scientific and practical conference]. Saint-Petersburg, 2020, pp. 237–241 (in Russian).

32. Aliyev T. I. *Osnovy modelirovanija diskretnyh sistem* [Fundamentals of modeling discrete systems]. Saint-Petersburg, St. Petersburg State University ITMO Publ., 2009. 363 p. (in Russian).

33. Chudnov A. M. *Matematicheskie osnovy modelirovanija, analiza i sinteza sistem* [Mathematical foundations of modeling, analysis and synthesis of systems]. Saint-Petersburg, Military Academy of Communications Publ., 2021. 192 p. (in Russian).

34. Thomas L. Saaty. *Mathematical Models of Arms Control and Disarmament: Applications of Mathematical Structures in Politics.* New York: John Wiley & Sons, 1968. 190 p.

35. Novikov D. A. *Teorija upravlenija organizacionnymi sistemami* [Theory of management of organizational systems]. Moscow, Moscow Psychological and Social Institute Publ., 2005. 584 p. (in Russian).

36. Lipatnikov V. A., Parfirov V. A. *Puti povyshenija adekvatnosti modelirovanija razvedyvatel'noj zashhishhennosti ob#ektov Vooruzhennyh sil. Voennaja bezopasnost' Rossii: vzgljad v budushhee. Materialy 8-j Mezhdunarodnoj mezhvedomstvennoj nauchno-prakticheskoj konferencii* [Ways to improve the adequacy of modeling the intelligence security of objects of the Armed Forces. Military Security of Russia: a Look into the Future. Materials of the 8th International Interdepartmental Scientific and Practical Conference]. Moscow, Publishing House of Bauman Moscow State Technical University, 2023, pp. 343–349 (in Russian).

37. Akinshin R. N., Anishchenko A. V., Ashurbeyli I. R. *Models of technical intelligence and threats to information security: Monograph*. Ed. E. M. Sukharev. Moscow, Radio Engineering, 2003. 142 p. (in Russian).

38. Lipatnikov V. A., Parfirov V. A. *Verojatnostno-vremennye pokazateli processa vyjavlenija setej radiosvjazi. Innovacionnye tehnologii i tehnicheskie sredstva special'nogo naznache-nija: Trudy XV nauchno-prakticheskoj konferencii* [Probabilistic-temporal indicators of the process of identifying radio communication networks. Innovative technologies and technical means of special purpose: Proceedings of the XV scientific and practical conference]. Saint-Petersburg, Baltic State Technical University "Voenmeh", 2023, pp. 172–175 (in Russian).

39. Barabash Y. L. *Collective statistical solutions in recognition*. Moscow, Radio i svjaz' Publ., 1983. 224 p. (in Russian).

40. Mazurov V. D. *Mathematical methods of pattern recognition. Study guide. 2nd ed., additional and revised.* Yekaterinburg, Ural State University named after A.M. Gorky Publ., 2010. 101 p. (in Russian).

41. Bronstein I. N., Semendyaev K. A. *Handbook of mathematics for engineers and students of higher education institutions. 13th ed., revised*. Moscow, Nauka Publ., 1986. 544 p. (in Russian).

42. Kushnir F. V. *Electrical and radio measurements.* Leningrad, Energoatomizdat Publ., 1983. 320 p. (in Russian).

43. Lipatnikov V. A., Parfirov V. A., Petrenko M. I. *Obshhij algoritm dinamicheskogo upravlenija ustojchivym funkcionirovaniem seti svjazi special'nogo naznachenija. Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii. XII Mezhdunarodnaja nauchno-tehnicheskaja i nauchno-metodicheskaja konferencija* [General algorithm of dynamic control of stable functioning of a special-purpose communication network. Actual problems of infotelecommunications in science and education. XII International Scientific-technical and scientific-methodological Conference]. Saint-Petersburg, 2023, pp. 814–819 (in Russian).

44. Voronov E. M., Karpunin A. A. Algorithms of hierarchical optimization in a two-level multichannel problem "management-regulation". *Bulletin of the Peoples' Friendship University of Russia. Series: Engineering Research*, 2009, no. 4, pp. 55–67 (in Russian).

45. Lipatnikov V. A., Parfirov V. A. Model of the process of observing multiple sources of information in stochastic conditions. *Informatsiya i kosmos*, 2022, no. 1, pp. 35–44 (in Russian).

46. Parfirov V. A. Mathematical model of the dynamics of movements of a locally distributed group object. *Enginery Problems. Series16. Anti-Terrorist Engineering Means*, 2022, vol. 171–172, no. 9–10, pp. 50–57 (in Russian).

47. Lipatnikov V. A., Sakharov D. V., Parfirov V. A., Petrenko M. I. *Modelirovanie funkcionirovanija raspredelennogo ob#ekta radiokontrolja. Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov Jubilejnoj XVIII Sankt-Peterburgskoj mezhdunarodnoj konferencii* [Modeling the functioning of a distributed objects of radio control. Regional informatics and information security. Proceeding of the jubilee XVII Saint-Petersburg]. Saint-Petersburg, 2022, pp. 599–604 (in Russian).

48. Lipatnikov V. A., Parfirov V. A. *Sposob modelirovanija mestonahozhdenija ob#ektov gruppy s uchetom dinamiki peremeshhenij. Innovacionnaja dejatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii* [A method for modeling the location of group objects taking into account the dynamics of movements. Innovative activity in the Armed Forces of the Russian Federation: Proceedings of the All-Army Scientific and Practical Conference]. Saint-Petersburg, 2022, pp. 253–258 (in Russian).

49. Lipatnikov V. A., Parfirov V. A. *Verojatnostnye harakteristiki processa opredelenija mestopolozhenija ob#ektov radiokontrolja s uchetom stohastichnosti parametrov izluchenij i pomeh. Aktual'nye problemy zashhity i bezopasnosti. Trudy XXV Vserossijskoj nauchno-prakticheskoj konferencii* [Probabilistic characteristics of

the process of determining the location of radio monitoring objects, taking into account the stochasticity of radiation and interference parameters. Actual problems of protection and security: Proceedings of the XXV All-Russian Scientific and Practical Conference, Saint-Petersburg]. Saint-Petersburg, 2022, pp. 299–304 (in Russian).

50. Lipatnikov V. A., Parfirov V. A. *Verojatnostno-vremennye harakteristiki processa izmerenija koordinat robototehnicheskih kompleksov voennogo naznachenija po izluchaemym radiosignalam. Perspektivnye sistemy i zadachi upravlenija: sbornik trudov XVII Vserossijskoj konferencii* [Probabilistic-temporal characteristics of the process of measuring the coordinates of military robotic complexes by radiated radio signals. Promising management systems and tasks: Proceedings of the XVII All-Russian Conference]. Taganrog, 2022, pp. 214–220 (in Russian).

51. Lipatnikov V. A., Parfirov V. A., Melekhov K. V. *Model' opredelenija verojatnostno-vremennyh harakteristik obnaruzhenija ob#ektov pri neodnokratnom obsledovanii mestnosti. Aktual'nye problemy zashhity i bezopasnosti: Trudy XXVI Vserossijskoj nauchno-prakticheskoj konferencii* [A model for determining the probabilistic-temporal characteristics of object detection during repeated terrain survey. Actual problems of protection and safety: Proceedings of the XXVI All-Russian Scientific and Practical Conference]. Saint-Petersburg, 2023, pp. 563–568 (in Russian).

52. Syzrantsev G. V. *Teoreticheskie i nauchno-metodicheskie osnovy obespechenija postroenija slozhnyh organizacionno-tehnicheskih sistem voennoj svjazi v lokal'nyh vojnah i vooruzhennyh konfliktah: Monografija* [Theoretical and scientific and methodological foundations for ensuring the construction of complex organizational and technical systems of military communications in local wars and armed conflicts: Monograph]. Edited by Professor A. G. Ermishyan. Saint-Petersburg, Military Academy of Communications Publ., 2007. 180 p. (in Russian).

53. Gurin L. S., Dymarsky Ya. S., Merkulov A. D. *Zadachi i metody optimal'nogo raspredelenija resursov* [Tasks and methods of optimal resource allocation]. Moscow, Sovetskoe radio Publ. 1968. 463 p. (in Russia).

54. Berzin E. A. *Optimal'noe raspredelenie resursov i teorija igr* [Optimal resource allocation and game theory]. Moscow, Radio i svjaz' Publ., 1983. 216 p. (in Russian).

55. Berzin E. A. *Optimal'noe raspredelenie resursov i jelementy sinteza sistem* [Optimal resource allocation and elements of systems synthesis]. Moscow, Sovetskoe radio Publ, 1974. 304 p. (in Russian).

56. Mikhailov R. L., Polyakov S. L. Optimal resource allocation model and research of information conflict strategies. *Systems of Control, Communication and Security*, 2018, no. 4, pp. 323–344 (in Russian).

57. Moiseev N. H., Ivanilov Yu. P., Stolyarova E. M. *Metody optimizacii* [Optimization methods]. Moscow, Nauka Publ., 1978. 352 p. (in Russian).

58. Busov V. I. *Upravlencheskie reshenija* [Managerial decisions]. Moscow, Izdatel'stvo Jurajt Publ., 2019. 254 p. (in Russian).

59. Ermishyan A. G. *Teoreticheskie osnovy postroenija sistem voennoj svjazi v ob#edinenijah i soedinenijah: Ch. 1. Metodologicheskie osnovy postroenie*

organizacionno-tehnicheskih sistem voennoj svjazi [Theoretical foundations of building military communications systems in associations and formations: Part 1. Methodological foundations of building organizational and technical systems of military communications]. Saint-Petersburg, Military Academy of Communications Publ., 2005. 740 p. (in Russian).

60. Dmitryuk A. M., Kasanin S. N., Gradusov R. A., Antonenko I. V. *Osnovy organizacii svjazi* [Fundamentals of communication organization]. Minsk: Belorusskij Gosudarstvennyj Universitet informatiki i radiojelektroniki Publ., 2012. 150 p. (in Russian).

61. Altukhov P. K., Afonsky I. A., Rybolovskij I. V., Tatarchenko A. E. *Osnovy teorii upravlenija vojskami* [*Fundamentals of the theory of command and control*]. Ed. Altukhova P K. Moscow, Voenizdat Publ., 1984. 221 p. (in Russian).

62. Lipatnikov V. A., Sakharov D. V., Parfirov V. A., Petrenko M. I. *Imitacionnaja model' raspredelennogo ob#ekta radiokontrolja, otrazhajushhaja dinamiku peremeshhenij i smenu rezhimov raboty radiojelektronnyh sredstv. Regional'naja informatika (RI-2022): Jubilejnaja XVIII Sankt-Peterburgskaja mezhdunarodnaja konferencija* [Simulation model of a distributed radio monitoring object reflecting the dynamics of movements and the change of modes of operation of radio-electronic means. Regional Informatics (RI-2022): Jubilee XVIII St. Petersburg International Conference. Materials of the conference]. Saint-Petersburg, 2022, pp. 556–558 (in Russian).

Статья поступила 8 сентября 2023 г.

Информация об авторах

Липатников Валерий Алексеевич – доктор технических наук, профессор. Старший научный сотрудник научно-исследовательского центра. Военная академия связи имени Маршала Советского Союза С.М. Буденного. Заслуженный изобретатель Российской Федерации. Почетный работник высшего профессионального образования Российской Федерации. Член-корреспондент Российской академии естественных наук. Область научных интересов: теория многоуровневой иерархической радиоэлектронной защиты, безопасности связи и информации инфотелекоммуникационных сетей. E–mail: lipatnikovanl@mail.ru

Парфиров Виталий Александрович – кандидат технических наук. Докторант. Военная академия связи имени Маршала Советского Союза С.М. Буденного. Область научных интересов: теория защиты от технических разведок; численная электродинамика. E–mail: vitaly.parfirov@yandex.ru

Адрес: 194064, Россия, г. Санкт-Петербург, Тихорецкий пр., д. 3.

Structural-parametric method of protection of information and telecommunication network of special purpose in the conditions of information conflict

V. A. Lipatnikov, V. A. Parfirov

Purpose. *Increasing the security of the special purpose information and telecommunication network (SP ITN) in the conditions of information conflict by operational management of structural and functional parameters of the elements.* ***Methods.*** *The solution of the problem is based on the joint application of methods of conflict theory, system analysis theory, set theory, control theory, optimization theory, modeling theory and combinatorics.* ***Novelty.*** *The proposed method is the development of the theory of management methods of SP ITN, the novelty elements of the presented solution consist in the use of additional source data, taking into account the data of forecasting the dynamics of their changes in the process of conflict development, which increases the accuracy of the assessment of time and probabilistic parameters of security when forming a model of changes in the security indicators of elements of SP ITN, as well as taking into account the impact of the selected actions when making decisions on changing the structural and functional parameters of elements during the information confrontation.* ***Results.*** *The use of the proposed method makes it possible to increase the efficiency and validity of responding to changes in the situation when managing the security of SP ITN by monitoring and predicting the current values of time and probabilistic indicators, as well as the process of developing scientifically sound solutions for managing the structural and functional parameters of the elements of SP ITN. Based on the results of the modeling of the method, its adequacy and extended functionality were confirmed.* ***Practical relevance.*** *The presented applied results can be implemented in the form of special software for information and analytical complexes in decision support systems for the protection of SP ITN. In addition, the proposed method can be used in the creation of intelligent control systems of a new generation, not only SP ITN, but also in the proactive management of other technical systems operating in conditions of information conflict.*

Key words: *information and telecommunication network, security, management, conflict, algorithm, dynamics of change, monitoring and intelligence system, resource management.*

Information about Authors

Valery Alekseevich Lipatnikov – Dr. habil. of Engineering Sciences, Full Professor. Senior Research Officer at the Research Center. Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. Honored Inventor of the Russian Federation. Honorary Worker of Higher Professional Education of the Russian Federation. Corresponding member of the Russian Academy of Natural Sciences. Research interests: theory of multilevel hierarchical electronic protection, communication and information security of infotelecommunication networks. E–mail: lipatnikovanl@mail.ru

Vitaly Alexandrovich Parfirov – Ph.D. of Engineering Sciences. Doctoral Candidate. Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. Research interests: theory of protection from technical intelligence; numerical electrodynamics. E–mail: vitaly.parfirov@yandex.ru

Address: Russia, 194064, Saint-Petersburg, Tihoreckiy prospekt, 3.