УДК 519.876

Обеспечение конфликтной устойчивости программной реализации алгоритмов управления радиоэлектронной аппаратурой пространственно распределенных организационно-технических систем

Бойко А. А., Будников С. А.

Постановка задачи. *В антагонистическом конфликте пространственно распределенных разнородных организационно-технических систем процессы функционирования радиоэлектронной аппаратуры многообразны, вариативны и трудно предсказуемы. Качество программной реализации алгоритмов управления радиоэлектронной аппаратурой оказывает существенное влияние на возможности таких систем. Однако известные методы синтеза организационно-технических систем это влияние не учитывают.* ***Цель работы:*** *обеспечить конфликтную устойчивость программной реализации алгоритмов управления радиоэлектронной аппаратурой организационно-технических систем.* ***Идея:*** *предлагается метод, состоящий в выявлении внешних и внутренних программных угроз безопасности заданного образца радиоэлектронной аппаратуры, специфичных для его телекоммуникационных протоколов и программных человеко-машинных интерфейсов, и определении тех угроз, устранение которых обеспечит повышение или достижение требуемого уровня целевой эффективности его организационно-технической системы в конфликте.* ***Новизна****: получена возможность оценки влияния качества программной реализации алгоритмов управления радиоэлектронной аппаратурой на ход и исход антагонистического конфликта организационно-технических систем, в котором эта аппаратура используется.* ***Результат****: предложенный метод трансформируется в методики обоснования численных значений параметров функциональной пригодности, производительности, надежности и защищенности программной реализации алгоритмов управления радиоэлектронной аппаратуры пространственно распределенных разнородных организационно-технических систем. Показан пример применения методики обоснования требований к функциональной пригодности программной реализации алгоритмов управления радиоэлектронной аппаратурой для боя двух равных батальонов при различных уровнях их информатизации* Δ*. Установлено, что функциональная пригодность программной реализации алгоритмов управления радиоэлектронной аппаратурой батальона в обороне должна быть не менее 0,32 при* $\Delta=0,5$*, не менее 0,53 при* $\Delta=0,6$*, не менее 0,65 при* $\Delta=0,7$*, не менее 0,72 при* $\Delta=0,8$*, не менее 0,77 при* $\Delta=0,9$ *и не менее 0,81 при* $\Delta=1$*.* ***Практическая значимость****: решение можно использовать при модернизации существующих и создании перспективных образцов конфликтно-устойчивой радиоэлектронной аппаратуры.*

Ключевые слова: *радиоэлектронная аппаратура, антагонистический конфликт, устойчивость, организационно-техническая система, программная угроза, алгоритм управления.*

Актуальность

В антагонистическом конфликте процессы функционирования, в том числе информационного взаимодействия, радиоэлектронной аппаратуры (РЭА) пространственно распределенных разнородных организационно-технических

Библиографическая ссылка на статью:
Бойко А. А., Будников С. А. Обеспечение конфликтной устойчивости программной реализации алгоритмов управления радиоэлектронной аппаратурой пространственно распределенных организационно-технических систем // Системы управления, связи и безопасности. 2019. № 4. С. 100-139. DOI: 1024411/2410-9916-2019-10404

Reference for citation:
Boyko A. A., Budnikov S. A. Conflict Resistance Ensuring of Software Implementation of Control Algorithms of Radioelectronic Equipment of Spatially Distributed Organization and Technical Systems. *Systems of Control, Communication and Security*, 2019, no. 4, pp. 100-139. DOI: 1024411/2410-9916-2019-10404 (in Russian).

систем (далее – ОТС) отличаются многообразием, вариативностью и низкой предсказуемостью. Такая РЭА может выступать в качестве самостоятельного элемента ОТС или его составной части и представляет собой систему или комплекс информационно-технических средств (ИТС), то есть радиоэлектронных средств, средств вычислительной техники и их конструктивно единых комбинаций с другими классами технических средств [1]. В конфликте аппаратура подвержена угрозам безопасности. Каждая угроза – это совокупность условий и факторов, создающих возможность нанести с использованием РЭА ущерб ОТС, в состав которой данная аппаратура входит. Наиболее полный перечень факторов, влияющих на безопасность РЭА и обрабатываемой с ее использованием информации, приведен в ГОСТ [2]. В рассматриваемом виде конфликта основными из этих факторов до недавнего времени являлись дефекты, сбои, отказы и аварии технического обеспечения, ошибки эксплуатирующих его операторов, диверсия (захват), огневое поражение, определяющих *физические угрозы безопасности* РЭА, а также разведка, уничтожение, блокирование информации с применением средств радиоэлектронного подавления (РЭП), поражения мощным электромагнитным излучением (ЭМИ), дезинформация (путем имитации обстановки), способствующая нецелевому использованию ресурсов самой РЭА и элементов своей ОТС, зависящих от результатов применения РЭА, определяющих *нецифровые информационные угрозы безопасности* РЭА.

Внедрение в РЭА последних достижений цифровых информационных и телекоммуникационных технологий добавило принципиально новые факторы, угрожающие ее безопасности. Ими стали дефекты, сбои и отказы программного обеспечения, ошибки персонала, эксплуатирующего программное обеспечение, в том числе эксплуатирующего средства и системы защиты информации, техническая компьютерная разведка, искажение, уничтожение или блокирование информации с применением средств программного воздействия (ПВ). Угрозы, связанные с этими новыми факторами, можно назвать *программными (или цифровыми информационными) угрозами безопасности* РЭА, поскольку все они обусловлены недостаточно высоким качеством программной реализации ее алгоритмов управления (АЛУ) (см., например, [3, 4]).

Качество программной реализации АЛУ наиболее полно характеризуется согласно ГОСТ [5] следующими показателями: 1) удобство использования, 2) переносимость (мобильность), 3) сопровождаемость (модифицируемость), 4) совместимость, 5) функциональная пригодность, 6) производительность, 7) надежность и 8) защищенность. На сегодняшний день в процессе разработки РЭА обеспечивается достаточно высокий уровень первых четырех из этих показателей, поскольку необходимые для этого меры интуитивно понятны и относительно просты. Остальные показатели существенно зависят не только от специфики организации работы заказчиков и ресурсной оснащенности разработчиков РЭА в каждом конкретном случае, но и от применяемых подходов к программной реализации АЛУ. К тому же на практике качеству программной реализации АЛУ часто не уделяется достаточное внимание, поскольку традиционно у разработчиков оно сосредоточено на техническом обеспечении РЭА, а программная реализация АЛУ доводится до стадии успешной отработки кон-

трольных примеров и дорабатывается по замечаниям пользователей в процессе эксплуатации. Показатели функциональной пригодности, надежности и производительности программной реализации АЛУ характеризуют область *внутренних программных угроз*, а защищенность – как внутренние программные угрозы, связанные с ошибками (в том числе умышленными) операторов, так и *внешние программные угрозы*, связанные с ПВ противостоящей ОТС.

Наличие большого числа программных угроз безопасности существующих и перспективных образцов РЭА на сегодняшний день является следствием *противоречия в практике* между потребностью в высоком уровне информатизации этих образцов и одновременно низким качеством программной реализации алгоритмов управления ими, не позволяющим в полной мере реализовать возможности их ОТС в конфликтных условиях. Устранение этого противоречия является одним из ключевых направлений совершенствования РЭА.

Постановка задачи

Наиболее яркими примерами антагонистического конфликта являются боевые действия и антитеррористические акции. Очевидно, что при введении ограничений на реализацию физических угроз безопасности РЭА в процессе взаимного влияния сторон антагонизм переходит в строгий конфликт. Строгий конфликт ОТС характерен, например, для борьбы коммерческих организаций за ограниченный и высокодоходный ресурс, а также для так называемого «периода непосредственной угрозы агрессии», когда отдельные страны или коалиции скрытно наносят друг другу максимально допустимый ущерб, дающий стратегическое преимущество и возможность достижения своих целей без перехода к открытой конфронтации. В настоящей работе объектом исследования является антагонистический конфликт ОТС, который иллюстрируется в основном примерами из области военного дела, но результаты работы могут распространяться и на строгий конфликт.

Согласно основному принципу теории эффективности целенаправленных процессов [6] в антагонистическом конфликте все элементы ОТС должны рассматриваться как образующие единое целое, помещенное в общую для конфликтующих сторон окружающую среду. При этом взаимодействие элементов каждой ОТС должно рассматриваться в условиях полномасштабного влияния противостоящей ОТС (далее – противника). Такое влияние, очевидно, должно учитывать процессы функционирования различных образцов РЭА, а также качество программной реализации их АЛУ, на которое оказывают существенное влияние внешние и внутренние программные угрозы безопасности. Однако указанные аспекты конфликтного взаимодействия в процессе синтеза конфликтно-устойчивых ОТС [7, 8], структура которого приведена на рис. 1, в настоящее время не учитываются. Это связано с недостаточно глубокой теоретической проработкой следующих научных направлений.

1. Научное направление **оценки качества программной реализации алгоритмов управления РЭА в условиях внешних программных угроз** (стрелка 1 на рис. 1) активно развивается с конца XX века в [9-37] и др. Оно имеет в основном фактографический базис, ядро которого составляют сведения об

успешной реализации внешних программных угроз безопасности РЭА и закономерности распространения в компьютерных сетях ОТС специальных программных средств (СПС), используемых в ходе ПВ. В этом направлении требуется дополнительная проработка вопросов синтеза полного множества тестовых способов реализации внешних программных угроз безопасности РЭА для заданной процедуры телекоммуникационного протокола. Сейчас для этого используется в основном эвристический метод, в котором процесс разработки тестовых способов не имеет четкого математического обоснования и состоит в поиске экспертом единичных тестовых способов нарушения штатного режима работы ИТС в специфических условиях и формировании настроенных только на данные способы средств защиты. Поэтому такой подход не позволяет полноценно парировать внешние программные угрозы безопасности РЭА. В данном направлении также отсутствуют модели процесса распространения СПС в компьютерных сетях, позволяющие анализировать конфликтную устойчивость ОТС (стрелка 4 на рис. 1), применяющих РЭА, на основе определения вероятностно-временных характеристик состояний каждого узлового ИТС сети с учетом ее архитектуры, поведенческих характеристик СПС и подсистем защиты информации узловых ИТС и возможности заражения множества узлов различными типами СПС.

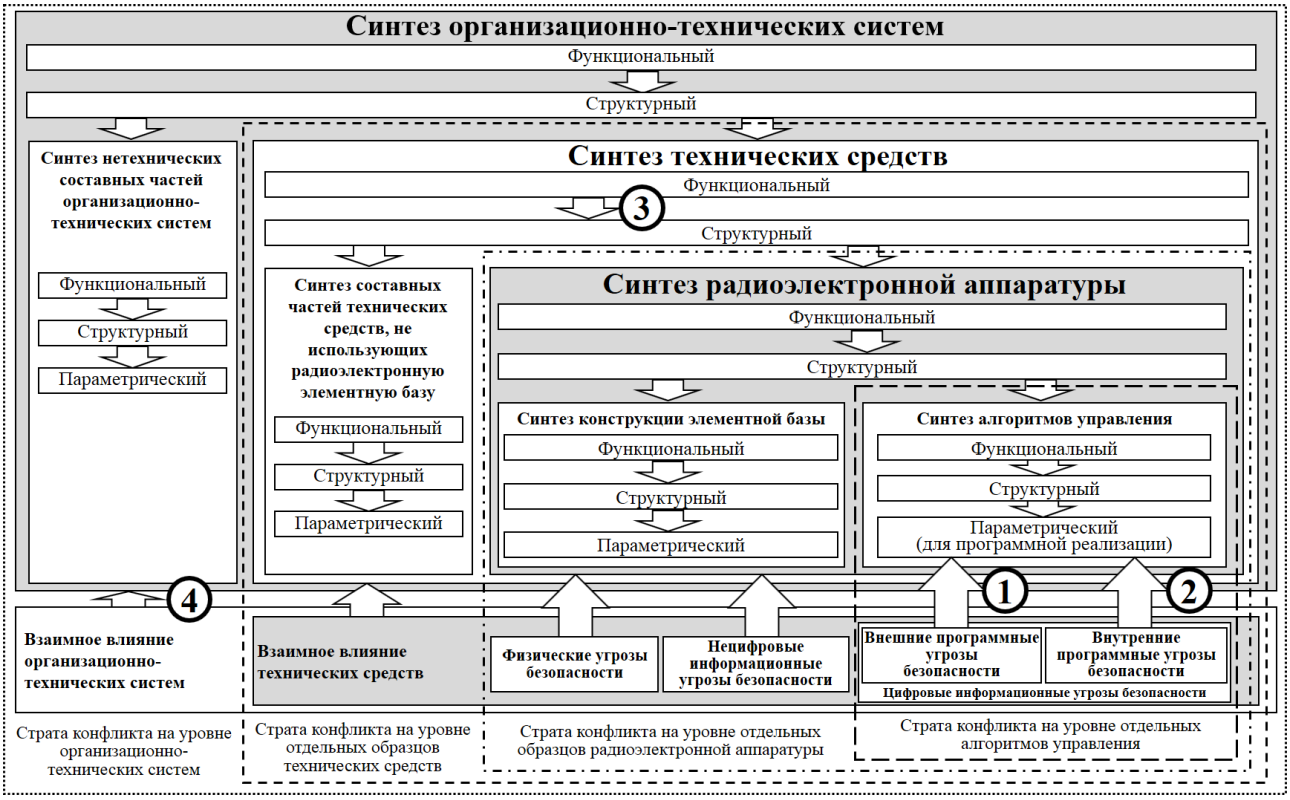

Рис. 1. Структура процесса синтеза конфликтно-устойчивых ОТС

2. Научное направление **оценки качества программной реализации алгоритмов управления РЭА в условиях внутренних программных угроз** (стрелка 2 на рис. 1) зародилось в 70-х годах XX века и освещено в работах [38-52] и др. В рамках данного направления качественные характеристики про-

граммной реализации АЛУ детально изучены с позиции «белого ящика», когда имеется достаточное для ее анализа время. Но модель жизненного цикла РЭА, часто применяемая разработчиками, предполагает скорейшую передачу заказчику окончательного результата разработки. В таких условиях применимы только т.н. методы «черного ящика», которые ориентированы на оценку качества программного человеко-машинного интерфейса РЭА. Однако известные подходы к оценке качества программной реализации АЛУ с позиции «черного ящика» не обеспечивают полноту множества путей тестирования потоков управления и данных в программном человеко-машинном интерфейсе, а также учет последовательностей выполнения задач РЭА в соответствии с их причинно-следственными связями.

3. Научное направление **синтеза конфликтно-устойчивой РЭА** известно с 60-х годов XX века из работ [53-70] и др. Положения, сформулированные в рамках данного направления и образующие самостоятельную теорию информационного конфликта РЭА, ориентированы на исследование дуэлей типа «отдельный образец технического средства с исследуемой РЭА – противостоящий образец технического средства с РЭА или без нее», либо их упрощенного варианта – дуэлей типа «исследуемый образец РЭА – другие образцы РЭА (своей и/или противостоящей ОТС)» (стрелка 3 на рис. 1). При этом в обоих типах дуэлей не учитываются условия конфликта сложных гетерогенных ОТС как единого целого, в котором применяются разнородные по своим задачам и используемым физическим принципам технические средства. Особенностью этого направления является то, что в нем программные реализации АЛУ в качестве объекта исследований до настоящего времени рассматривались только с позиции повышения их производительности.

4. Научное направление **моделирования антагонистического конфликта ОТС** (стрелка 4 на рис. 1) известно, в первую очередь, в военном деле со времен Архимеда [71]. Оно развито в работах [71-90] и др. Однако применение известных в данном направлении подходов не обеспечивает возможность анализа особенностей функционирования РЭА разнородных элементов ОТС. Также в рамках этого направления не учитывается взаимное влияние всей совокупности функций разнородных элементов конфликтующих ОТС (например, для вооруженного конфликта это функции огневого поражения, разведки, управления, связи, РЭП, ПВ, имитации обстановки, поражения ЭМИ, радиационного, химического, биологического, нелетального и психологического воздействия). Под однородностью элементов ОТС здесь подразумевается их нахождение в состоянии непосредственной дуэли друг с другом. Например, бой двух танковых формирований, бой танкового формирования с формированием, оснащенным противотанковыми средствами, конфликт средств связи одного формирования со средствами радиоэлектронной борьбы другого формирования. Важно отметить, что на сегодняшний день в рамках исследований по этому направлению структура ОТС формируется в основном эмпирически, наполняясь по мере потребности отдельными элементами, для которых впоследствии решается проблема «бесшовной» связи с ранее добавленными элементами.

С учетом вышеизложенного взаимное влияние ОТС в антагонистическом конфликте можно представить в виде схемы, показанной на рис. 2. На ней пунктиром выделено влияние, которое сегодня оценивается только экспертами.

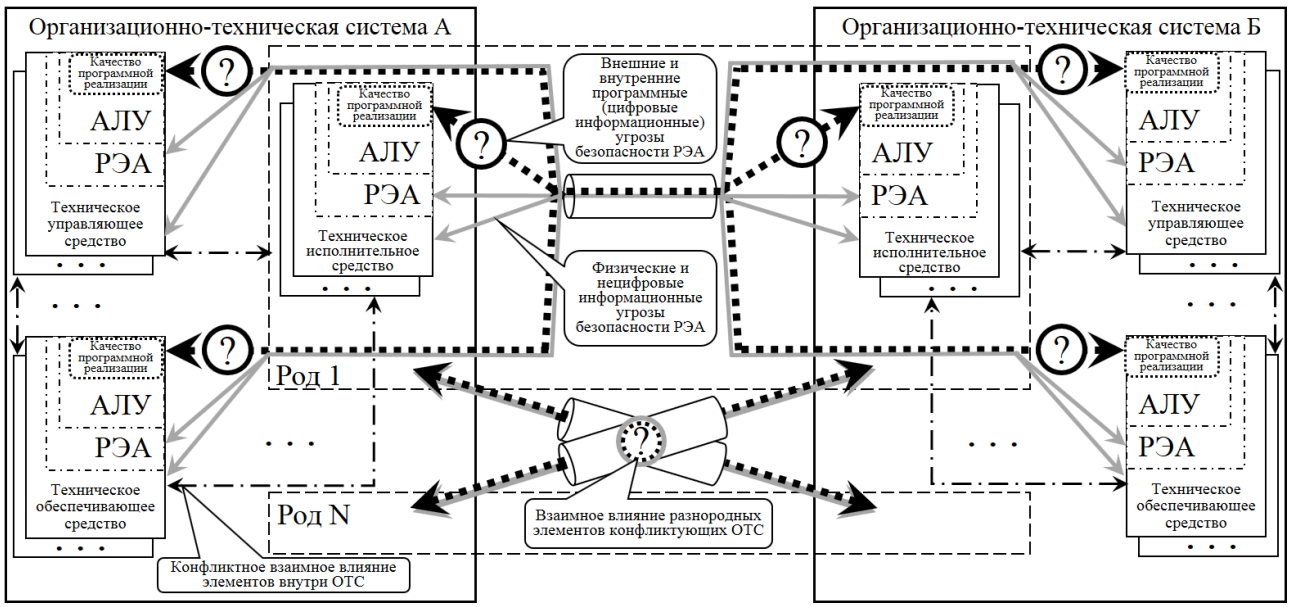

Рис. 2. Структурная схема антагонистического конфликта ОТС

Данные обстоятельства свидетельствуют об актуальном для создания перспективных и модернизации существующих образцов РЭА *противоречии в науке* между потребностью в методиках оценки влияния программных угроз РЭА на целевую эффективность ОТС в антагонистическом конфликте и недостаточной развитостью методов синтеза конфликтно-устойчивых ОТС.

Цель работы – обеспечение конфликтной устойчивости программной реализации алгоритмов управления радиоэлектронной аппаратурой пространственно распределенных разнородных организационно-технических систем.

Содержание метода

Для достижения указанной цели предлагается метод, базирующийся на последовательном решении следующих научных задач:

1) исследование процессов функционирования РЭА вне конфликта ОТС в условиях реализации программных угроз ее безопасности;
2) выявление множества программных угроз безопасности заданного образца РЭА, специфичных для его телекоммуникационных протоколов и программных человеко-машинных интерфейсов;
3) исследование конфликта ОТС, применяющих РЭА;
4) определение тех программных угроз безопасности заданного образца РЭА, устранение которых обеспечит повышение или достижение требуемого уровня целевой эффективности его ОТС в конфликте.

Рассмотрим постановки этих задач по схеме, изложенной в [91, 92].

Задача 1. Даны следующие конечные множества.

1. I – непустое множество образцов РЭА в ОТС, включающее заданный образец РЭА и все образцы РЭА, с которыми он взаимодействует.

2. J_i – непустое множество образцов ИТС в i-м образце РЭА ($i = 1\ldots|I|$, где $|\ldots|$ – мощность множества, $J = \bigcup_{\forall i} J_i$).

3. $S_{i,j} = \{s_{i,j,\mu}\}$, где $j = 1\ldots|J_i|$, $\mu = 1\ldots|S_{i,j}|$ – непустое множество *процессов функционирования* программной реализации АЛУ j-м ИТС i-го образца РЭА ($S = \bigcup_{\forall i,j} S_{i,j}$). Критерии формирования процессов ИТС приведены в [93]. Совокупность этих критериев позволяет сформировать множество корректных процессов $S^{\sim}$, т.е. $S \subseteq S^{\sim}$. Этап процесса ИТС может включать *прием/передачу сообщения*, а также использовать *программный человеко-машинный интерфейс* (далее – интерфейс) для взаимодействия с оператором. Интерфейс – это совокупность программных средств, обеспечивающих диалог человека-оператора с ИТС и визуализацию виртуальных объектов на экране его дисплея. Процесс, в котором содержится прием/передача некоторого множества сообщений, совместно с процессами других ИТС, от которых принимаются или которым передаются сообщения из этого множества, обеспечивает реализацию некоторой процедуры телекоммуникационного протокола.

4. $C_{i,j} = \{c_{i,j,\mu}\}$ – множество интерфейсов j-го ИТС i-го образца РЭА, $c_{i,j,\mu}$ – интерфейс μ-го процесса этого ИТС ($C = \bigcup_{\forall i,j} C_{i,j}$).

5. $NC = \bigcup_{\forall i,j,\mu} NC_{i,j,\mu}$: $NC_{i,j,\mu} = \left\{V_{i,j,\mu,n} \times T_{i,j,\mu,n}\right\}$, где $n = 1...|NC_{i,j,\mu}|$ – множество пар «действие-время», являющееся результатом декартова произведения следующих множеств:

- $V_{i,j,\mu,n} = V^{+}_{i,j,\mu,n} \cup V^{-}_{i,j,\mu,n} \subseteq V^{\sim}_{i,j,\mu,n}$, где: $V^{+}_{i,j,\mu,n}$ и $V^{-}_{i,j,\mu,n}$ – множества, соответственно, предусмотренных и непредусмотренных, в том числе умышленно ошибочных, действий человека-оператора с интерфейсом $c_{i,j,\mu}$; $V^{\sim}_{i,j,\mu,n}$ – множество действий с интерфейсом $c_{i,j,\mu}$, доступных человеку-оператору ($V^{+} = \bigcup_{\forall i,j,\mu,n} V^{+}_{i,j,\mu,n}$, $V^{-} = \bigcup_{\forall i,j,\mu,n} V^{-}_{i,j,\mu,n}$, $V^{\sim} = \bigcup_{\forall i,j,\mu,n} V^{\sim}_{i,j,\mu,n}$);
- $T_{i,j,\mu,n} = T^{+}_{i,j,\mu,n} \cup T^{-}_{i,j,\mu,n} \subseteq T^{\sim}_{i,j,\mu,n}$, где: $T^{+}_{i,j,\mu,n}$ и $T^{-}_{i,j,\mu,n}$ – множества, соответственно, предусмотренных и непредусмотренных моментов времени выполнения действий человека-оператора с интерфейсом $c_{i,j,\mu}$; $T^{\sim}_{i,j,\mu,n}$ – непустое множество допустимых моментов времени выполнения действий человека-оператора с интерфейсом $c_{i,j,\mu}$ ($T^{+} = \bigcup_{\forall i,j,\mu,n} T^{+}_{i,j,\mu,n}$, $T^{-} = \bigcup_{\forall i,j,\mu,n} T^{-}_{i,j,\mu,n}$, $T^{\sim} = \bigcup_{\forall i,j,\mu,n} T^{\sim}_{i,j,\mu,n}$).

Алгоритмы формирования множества NC изложены в [50, 94-96].

6. $M = \left\{m_{i,j,\mu,r}\right\}$, где $r = 1\ldots|M|$ – непустое множество типов сообщений, которыми обмениваются ИТС заданного i-го образца РЭА, где $m_{i,j,\mu,r}$ – r-й тип сообщения, используемый в μ-м процессе j-го ИТС заданного i-го образца РЭА.

7. $PV = \bigcup_{\forall i,j,\mu,r} PV_{i,j,\mu,r}$: $PV_{i,j,\mu,r} = \left\{ W_{i,j,\mu,r,k} \times \Omega_{i,j,\mu,r,k} \right\}$, где $k = 1 \ldots |PV_{i,j,\mu,r}|$ – множество пар «сообщение-время», являющееся результатом декартова произведения следующих множеств:

- $W_{i,j,\mu,r,k} = W^{+}_{i,j,\mu,r,k} \cup W^{-}_{i,j,\mu,r,k} \subseteq W^{\sim}_{i,j,\mu,r,k}$, где: $W^{+}_{i,j,\mu,r,k}$ и $W^{-}_{i,j,\mu,r,k}$ – множества, соответственно, предусмотренных и непредусмотренных телекоммуникационным протоколом вариантов содержания сообщения *r*-го типа μ-го процесса *j*-го ИТС *i*-го образца РЭА; $W^{\sim}_{i,j,\mu,r,k}$ – непустое множество допустимых телекоммуникационным протоколом вариантов содержания сообщения *r*-го типа в μ-м процессе *j*-го ИТС *i*-го образца РЭА ($W^{+} = \bigcup_{\forall i,j,\mu,r,k} W^{+}_{i,j,\mu,r,k}$, $W^{-} = \bigcup_{\forall i,j,\mu,r,k} W^{-}_{i,j,\mu,r,k}$, $W^{\sim} = \bigcup_{\forall i,j,\mu,r,k} W^{\sim}_{i,j,\mu,r,k}$);
- $\Omega_{i,j,\mu,r,k} = \Omega^{+}_{i,j,\mu,r,k} \cup \Omega^{-}_{i,j,\mu,r,k} \subseteq \Omega^{\sim}_{i,j,\mu,r,k}$, где: $\Omega^{+}_{i,j,\mu,r,k}$ и $\Omega^{-}_{i,j,\mu,r,k}$ – множества, соответственно, предусмотренных и непредусмотренных моментов времени передачи сообщения *r*-го типа в μ-м процессе *j*-го ИТС *i*-го образца РЭА; $\Omega^{\sim}_{i,j,\mu,r,k}$ – непустое множество моментов времени передачи сообщения *r*-го типа в μ-м процессе *j*-го ИТС *i*-го образца РЭА, длительность интервалов между которыми синхронизирована с каналом связи, обеспечивающим этот процесс ($\Omega^{+} = \bigcup_{\forall i,j,\mu,r,k} \Omega^{+}_{i,j,\mu,r,k}$, $\Omega^{-} = \bigcup_{\forall i,j,\mu,r,k} \Omega^{-}_{i,j,\mu,r,k}$, $\Omega^{\sim} = \bigcup_{\forall i,j,\mu,r,k} \Omega^{\sim}_{i,j,\mu,r,k}$).

Алгоритм формирования множества *PV* разработан в [93, 97].

8. $Y = \left\{ y_{i,j} \right\}$ – множество индикаторов работоспособности ИТС в заданном *i*-м образце РЭА. Элементы множества *Y* принимают следующие значения:

$$y_{i,j} = \begin{cases} 1, \text{ если } j\text{-е ИТС находится в штатном режиме после} \\ \quad \text{действия оператора с его интерфейсом или получения} \\ \quad \text{им одного или нескольких однотипных сообщений;} \\ 0 \text{ в противном случае.} \end{cases}$$

Под нештатным режимом понимается нахождение ИТС в одном из следующих состояний [97]: неработоспособное состояние, состояние сниженной производительности, состояние управляемости источником воздействия и состояние доступности для углубленного анализа источником воздействия.

Вариант структурной схемы процессов функционирования РЭА, соответствующий приведенным математическим абстракциям, показан на рис. 3.

В **задаче 1** требуется разработать детерминированную модель δ совокупности процессов функционирования заданного образца РЭА в ОТС, устанавливающую закономерность изменения множества *Y* выходных параметров от множеств V^{+}, T^{+}, W^{+}, Ω^{+} входных параметров, множеств *I*, *J*, *S*, *C*, *M* внутренних параметров и множеств V^{-}, T^{-}, W^{-}, Ω^{-} параметров конфликтных условий функционирования. При этом на множество *S* процессов функционирования ИТС, входящих в состав РЭА, накладывается ограничение корректности $S \subseteq S^{\sim}$, а на значения параметров множеств V^{+}, T^{+}, W^{+}, Ω^{+}, V^{-}, T^{-}, W^{-}, Ω^{-} накладываются

ограничения физической реализуемости: $V^+ \cup V^- \subseteq V^{\sim}$, $T^+ \cup T^- \subseteq T^{\sim}$, $W^+ \cup W^- \subseteq W^{\sim}$, $\Omega^+ \cup \Omega^- \subseteq \Omega^{\sim}$.

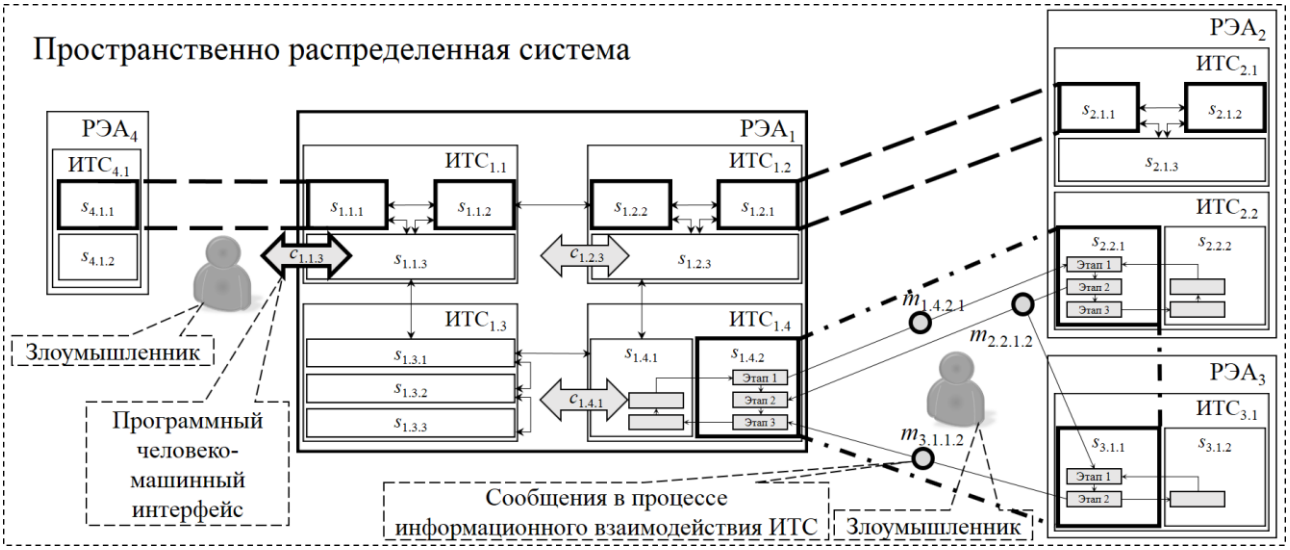

Рис. 3. Структурная схема процессов функционирования РЭА в ОТС (вариант)

Формальная постановка **задачи 1** имеет следующий вид:

$$\delta: \ \left\langle I, J, S, C, M, \left\{V^+ \cup V^- \times T^+ \cup T^-\right\}, \left\{W^+ \cup W^- \times \Omega^+ \cup \Omega^-\right\}\right\rangle \to Y$$

$$\text{при } S \subseteq S^{\sim},\ V^+ \cup V^- \subseteq V^{\sim},\ T^+ \cup T^- \subseteq T^{\sim},$$

$$W^+ \cup W^- \subseteq W^{\sim},\ \Omega^+ \cup \Omega^- \subseteq \Omega^{\sim}. \qquad (1)$$

Задача 2. Дана модель δ, см. выражение (1). Требуется выявить на основе модели δ два множества пар $\left\langle v \in V_{\text{сущ}}, t \in T_{\text{сущ}}\right\rangle$ и $\left\langle w \in W_{\text{сущ}}, \omega \in \Omega_{\text{сущ}}\right\rangle$ существенных значений параметров условий функционирования заданного образца РЭА при их варьировании на всем диапазоне допустимых значений: $v \in V^+ \cup V^-$, $t \in T^+ \cup T^-$, $w \in W^+ \cup W^-$, $\omega \in \Omega^+ \cup \Omega^-$. Критерием существенности значений пар параметров $\langle v, t\rangle$ и $\langle w, \omega\rangle$ является перевод при этих значениях любого из ИТС заданного *i*-го образца РЭА в нештатный режим, т.е. $\exists j: y_{i,j} = 0$.

Формальная постановка **задачи 2** состоит в следующем: на основе модели δ найти существенные параметры *j*-го заданного образца РЭА

$$\forall\, v, t, w, \omega \ \left(v \in V^+ \cup V^-, t \in T^+ \cup T^-, w \in W^+ \cup W^-, \omega \in \Omega^+ \cup \Omega^-\right):$$

$$v \in V_{\text{сущ}}, t \in T_{\text{сущ}}, \text{ если } \exists j: \quad y_{i,j}\left(I, J, S, C, M, \langle v, t\rangle, \langle W, \Omega\rangle\right) = 0;$$

$$w \in W_{\text{сущ}}, \omega \in \Omega_{\text{сущ}}, \text{ если } \exists j: \quad y_{i,j}\left(I, J, S, C, M, \langle V, T\rangle, \langle w, \omega\rangle\right) = 0. \qquad (2)$$

Задача 3. Даны следующие конечные множества.

1. U – кортеж метеорологических, географических и временны*ы*х условий конфликта.

2. $OB^{A(Б)}$ – кортеж непустых множеств параметров обеспечения конфликтующих ОТС. Например, множества параметров обеспеченности горюче-

смазочными материалами, боеприпасами, медицинскими и другими средствами. Здесь и далее верхний индекс *А* или *Б* означает сторону конфликта.

3. $N^{А(Б)} = \left\{ N_i^{А(Б)} \right\}$ – непустое множество элементов конфликтующих ОТС, где $N_i^{А(Б)}$ – кортеж параметров *i*-го элемента ОТС. Здесь и далее полагается, что в каждом *i*-м элементе ОТС используется только *i*-й образец РЭА. Кортеж $N_i^{А(Б)}$ включает:

$CT_i^{А(Б)} = \left\langle PE_i^{А(Б)}, RA_i^{А(Б)}, TS_i^{А(Б)} \right\rangle$ – кортеж множеств, как минимум одно из которых не пустое. В нем $PE_i^{А(Б)}$ – множество людей в *i*-м элементе (параметры уровня подготовки, наличие опыта и способности работать в команде, защищенности от влияния противника, выполняемые задачи, возможности влияния на противника в части обнаружения и распознавания его элементов), $RA_i^{А(Б)}$ – множество ИТС, образующих РЭА *i*-го элемента, $TS_i^{А(Б)}$ – множество нерадиоэлектронных технических средств (НТС), то есть не использующих радиоэлектронную элементную базу (параметры защищенности от влияния противника, потребных для работы ресурсов, времени подготовки к работе, выполняемых задач, надежности, возможностей по влиянию на противника), в *i*-м элементе ($PE^{А(Б)} = \bigcup_{\forall i} PE_i^{А(Б)}$, $RA^{А(Б)} = \bigcup_{\forall i} RA_i^{А(Б)}$, $TS^{А(Б)} = \bigcup_{\forall i} TS_i^{А(Б)}$);

- $P_i^{А(Б)}$ – непустое множество параметров, характеризующих местоположение *i*-го элемента;
- $G_i^{А(Б)}$ – множество параметров управления *i*-м элементом ОТС, определяемых программной реализацией алгоритмов управления РЭА (время обработки разведданных и донесений, принятия решения, формирования и отправки директивного документа, донесения, обработки и ретрансляции документа; уровень информатизации элемента, т.е. доля процессов, реализуемых с использованием РЭА, см. [98]);
- $L_i^{А(Б)}$ – множество параметров работы людей в *i*-м элементе ОТС (уровень подготовленности и опыта персонала, слаженность его работы);
- $Z_i^{А(Б)}$ – непустое множество параметров защищенности *i*-го элемента от влияния противника и своей ОТС;
- $B_i^{А(Б)}$ – непустое множество параметров подверженности диверсии *i*-го элемента со стороны противника (в целях добывания информации в элементе, использования элемента против его ОТС, уничтожения элемента и подмены информации в нем);
- $VP_i^{А(Б)}$ – непустое множество параметров, характеризующих время подготовки *i*-го элемента к работе;
- $H_i^{А(Б)}$ – непустое множество параметров, характеризующих уровень ущерба, который необходимо нанести *i*-му элементу для его вывода из строя ($P^{А(Б)} = \bigcup_{\forall i} P_i^{А(Б)}$, $B^{А(Б)} = \bigcup_{\forall i} B_i^{А(Б)}$, $H^{А(Б)} = \bigcup_{\forall i} H_i^{А(Б)}$, $L^{А(Б)} = \bigcup_{\forall i} L_i^{А(Б)}$,

$Z^{А(Б)} = \bigcup_{\forall i} Z_i^{А(Б)}$, $VP^{А(Б)} = \bigcup_{\forall i} VP_i^{А(Б)}$, $G^{А(Б)} = \bigcup_{\forall i} G_i^{А(Б)} \subseteq G^{\sim}$, где $G^{\sim}$ – множество ограничений на физическую реализуемость).

Кортеж $RA_i^{А(Б)}$ состоит из множеств, характеризующих следующие параметры *j*-го ИТС в *i*-м элементе: $ID_{i,j}^{А(Б)}$ – параметры защищенности от влияния противника; $IR_{i,j}^{А(Б)}$ – параметры потребного ресурса электрообеспечивающих средств; $IT_{i,j}^{А(Б)}$ – параметры времени подготовки к работе, определяемые программной реализацией АЛУ; $IV_{i,j}^{А(Б)}$ – параметры возможностей по влиянию на противника; $IP_{i,j}^{А(Б)}$ – параметры процессов функционирования ($IR^{А(Б)} = \bigcup_{\forall i,j} IR_{i,j}^{А(Б)}$, $IV^{А(Б)} = \bigcup_{\forall i,j} IV_{i,j}^{А(Б)}$, $IT^{А(Б)} = \bigcup_{\forall i,j} IT_{i,j}^{А(Б)} \subseteq IT^{\sim}$, где $IT^{\sim}$ – множество ограничений на физическую реализуемость).

Кортеж $ID_{i,j}^{А(Б)}$ состоит из множеств, характеризующих следующие параметры *j*-го ИТС в *i*-м элементе: $IDF_{i,j}^{А(Б)}$ – параметры защиты от огневого поражения; $IDE_{i,j}^{А(Б)}$ – параметры защиты от поражения ЭМИ; $IDR_{i,j}^{А(Б)}$ – параметры защиты от РЭП; $IDP_{i,j}^{А(Б)}$ – параметры защиты программной реализации АЛУ от ПВ (период и время смены параметров телекоммуникационных протоколов, период и время регламентного поиска СПС, время обнаружения активных СПС); $IDI_{i,j}^{А(Б)}$ – параметры защиты от разведки ($IDF^{А(Б)} = \bigcup_{\forall i,j} IDF_{i,j}^{А(Б)}$, $IDE^{А(Б)} = \bigcup_{\forall i,j} IDE_{i,j}^{А(Б)}$, $IDR^{А(Б)} = \bigcup_{\forall i,j} IDR_{i,j}^{А(Б)}$, $IDI^{А(Б)} = \bigcup_{\forall i,j} IDI_{i,j}^{А(Б)}$, $IDP^{А(Б)} = \bigcup_{\forall i,j} IDP_{i,j}^{А(Б)} \subseteq IDP^{\sim}$, где $IDP^{\sim}$ – множество ограничений на физическую реализуемость).

Кортеж $IP_{i,j}^{А(Б)}$ состоит из множеств, характеризующих следующие параметры *j*-го ИТС в *i*-м элементе: $IPZ_{i,j}^{А(Б)}$ – параметры выполняемых задач (приоритет, время выполнения, требуемая вычислительная мощность, интенсивность поступления); $IPT_{i,j}^{А(Б)}$ – параметры качества элементной базы (надежность и производительность); $IPA_{i,j}^{А(Б)} = \left\langle V_{i,j}^{А(Б)}, T_{i,j}^{А(Б)} \right\rangle \cup \left\langle W_{i,j}^{А(Б)}, \Omega_{i,j}^{А(Б)} \right\rangle$ – параметры процессов программной реализации АЛУ ($IPZ^{А(Б)} = \bigcup_{\forall i,j} IPZ_{i,j}^{А(Б)}$; $IPT^{А(Б)} = \bigcup_{\forall i,j} IPT_{i,j}^{А(Б)}$; $IPA^{А(Б)} = \bigcup_{\forall i} IPA_i^{А(Б)}$; $IPA_i^{А(Б)} = \bigcup_{\forall j} IPA_{i,j}^{А(Б)}$). Для заданного образца РЭА *i*-го элемента стороны А $\left\langle V_{\text{сущ}i}^{А}, T_{\text{сущ}i}^{А} \right\rangle = \bigcup_{\forall j} \left\langle V_{\text{сущ}i,j}^{А}, T_{\text{сущ}i,j}^{А} \right\rangle$, $\left\langle W_{\text{сущ}i}^{А}, \Omega_{\text{сущ}i}^{А} \right\rangle = \bigcup_{\forall j} \left\langle W_{\text{сущ}i,j}^{А}, \Omega_{\text{сущ}i,j}^{А} \right\rangle$ (см. решение **задачи 2**). Задачи ИТС условно могут быть разделены на четыре группы:

1) *информационные задачи*, обеспечивающие формирование запросов в базу данных и получение ответа от нее, а также представление информации в требуемом виде;
2) *расчетные задачи*, обеспечивающие ввод исходных данных для расчетов, их проведение и отображение результатов. Часто на практике имеют место информационно-расчетные задачи;
3) *телекоммуникационные задачи*, обеспечивающие связь (от лат. communico – делаю общим, связываю, общаюсь) ИТС с объектами, находящимся от него на удалении (от греч. tele – вдаль, далеко). Например, к таким задачам относятся разведка, передача данных, РЭП, поражение ЭМИ, ПВ, акустическое, психотронное воздействие;
4) *задачи управления*, обеспечивающие управление НТС или иным ИТС.

Совокупность условий физической реализуемости элементов конфликтующих ОТС характеризуется множеством $N^{\sim}$.

4. $R = \left\{ R_{\eta} \right\}, \eta = 1...\left| PE^{A} \times TS^{A} \times RA^{A} \times PE^{Б} \times TS^{Б} \times RA^{Б} \right|$ – множество элементов, характеризующих многоуровневое иерархически упорядоченное информационное взаимодействие и взаимное влияние ИТС, НТС и людей ОТС в конфликте. В состав кортежа $R_{\eta} = \left\langle TY_{\eta}, CH_{\eta} \right\rangle$ входят множества:

- TY_{η} – непустое множество типов связей в η-й паре ИТС, НТС и людей в конфликтующих ОТС. Типы связей: подчинение/управление, вхождение в состав элемента, информационное взаимодействие, деструктивное влияние;
- CH_{η} – непустое множество параметров, характеризующих каждую связь в η-й паре ИТС, НТС и людей в конфликтующих ОТС.

Совокупность условий физической реализуемости связей ИТС, НТС и людей ОТС в конфликте характеризуется множеством $R^{\sim}$.

5. F – множество значений показателя целевой эффективности ОТС, использующей заданный образец РЭА, в динамике конфликта.

В **задаче 3** требуется разработать детерминированную модель ξ процесса антагонистического конфликта ОТС, устанавливающую закономерность изменения элементов множества *F*, характеризующего динамику этого конфликта во множестве условий *U*, от множеств OB^{A}, $OB^{Б}$ входных параметров, множеств *R*, $N^{Б}$, N^{A} внутренних параметров в условиях влияния дестабилизирующих параметров функционирования $\left\langle V^{A}_{\text{сущ}\,i}, T^{A}_{\text{сущ}\,i} \right\rangle$ и $\left\langle W^{A}_{\text{сущ}\,i}, \Omega^{A}_{\text{сущ}\,i} \right\rangle$ для заданного образца РЭА *i*-го элемента ОТС стороны *A*. На множества *R*, $N^{A(Б)}$, $OB^{A(Б)}$, $G^{A(Б)}$, $IT^{A(Б)}$, $IDP^{A(Б)}$ накладываются условия физической реализуемости: $R \subseteq R^{\sim}$, $OB^{A(Б)} \subseteq OB^{\sim}$, $G^{A(Б)} \cup IT^{A(Б)} \cup IDP^{A(Б)} \subset N^{A(Б)} \subseteq N^{\sim}$.

Формальная постановка **задачи 3** имеет следующий вид:

$$\xi: \quad X \to F \text{ при } R \subseteq R^{\sim}, N^{A(Б)} \subseteq N^{\sim}, OB^{A(Б)} \subseteq OB^{\sim},$$

$$X = \left\langle \left\langle \left\langle PE^{A}, \left\langle \left\langle IDF^{A}, IDE^{A}, IDR^{A}, IDP^{A}, IDI^{A} \right\rangle, IR^{A}, IT^{A}, IV^{A}, \right. \right. \right. \right.$$

$$\left\langle IPZ^{A}, IPT^{A}, \left(IPA^{A} \setminus IPA_{i}^{A}\right) \cup \left\langle V_{\text{сущ}\,i}^{A}, T_{\text{сущ}\,i}^{A} \right\rangle \cup \left\langle W_{\text{сущ}\,i}^{A}, \Omega_{\text{сущ}\,i}^{A} \right\rangle \right\rangle, TS^{A} \Big\rangle,$$

$$P^{A}, G^{A}, L^{A}, Z^{A}, B^{A}, VP^{A}, H^{A} \big\rangle, N^{Б}, R, U, OB^{A}, OB^{Б} \Big\rangle. \quad (3)$$

Задача 4. Дана модель ξ, см. выражение (3). Требуется разработать метод Σ обеспечения заданного уровня $f_{\text{тр}}$ значения показателя целевой эффективности ОТС стороны *A*, применяющей заданный *i*-й образец РЭА, или максимизации значения этого показателя при недостижимости заданного уровня за счет варьирования значений параметров защиты программной реализации АЛУ в ИТС заданного образца РЭА от ПВ IDP_{i}^{A}, параметров времени подготовки этих ИТС к работе IT_{i}^{A} и параметров управления заданным образцом РЭА G_{i}^{A} в условиях влияния дестабилизирующих пар параметров функционирования $\left\langle V_{\text{сущ}i}^{A}, T_{\text{сущ}i}^{A} \right\rangle$ и $\left\langle W_{\text{сущ}i}^{A}, \Omega_{\text{сущ}i}^{A} \right\rangle$ этого образца РЭА в диапазоне их значений $IDP_{i}^{A} \subseteq IDP^{\sim}$, $IT_{i}^{A} \subseteq IT^{\sim}$, $G_{i}^{A} \subseteq G^{\sim}$ при заданных остальных параметрах кортежа N^{A}, кортежей $N^{Б}$, *R*, ресурсных ограничениях OB^{A}, $OB^{Б}$, стоимостных ограничениях $\Lambda_{\text{доп}}$ и условиях *U*.

Формальная постановка **задачи 4** имеет вид: найти метод Σ такой, что

$$\Sigma: \ \left\langle \xi, F, \beta \right\rangle \to \left\{ f_{a} \right\} \Big| \ \exists \left(a \in 1 \ldots \left| \Psi \right| \right)$$

$$\left(x_{a} = \underset{x_{a} \in X^{CT},\, X^{CT} \neq \varnothing}{\arg\min} \xi\left(x_{a}\right) \right) \vee \left(\left(x_{a} = \underset{x_{a} \in X,\, X^{CT} = \varnothing}{\arg\max} \xi\left(x_{a}\right) \right) \wedge \left(\beta\left(x_{a}\right) \le \Lambda_{\text{доп}} \right) \right)$$

$$\text{при} \left(x_{a} \in X^{CT} \right) = \left\{ x \in X \mid \ \left(\xi(x) \ge f_{\text{тр}} \right) \wedge \left(\beta(x) \le \Lambda_{\text{доп}} \right) \right\},$$

$$\Psi = IDP_{i}^{A} \times IT_{i}^{A} \times G_{i}^{A} \times \left\langle V_{\text{сущ}\,i}^{A}, T_{\text{сущ}\,i}^{A} \right\rangle \times \left\langle W_{\text{сущ}\,i}^{A}, \Omega_{\text{сущ}\,i}^{A} \right\rangle,$$

$$R \subseteq R^{\sim}, N^{A(Б)} \subseteq N^{\sim}, OB^{A(Б)} \subseteq OB^{\sim}, \quad (4)$$

где $\beta(x)$ – функция стоимости варианта параметров *x*.

Технологическая схема решения изложенных выше задач показана на рис. 4. Она состоит из блоков, характеризующих этапы метода. Рассмотрим их.

Этап 1. Исследование процессов функционирования РЭА вне конфликта в условиях реализации программных угроз ее безопасности с использованием:

- 1.1) модели информационного взаимодействия нескольких ИТС в рамках заданной процедуры телекоммуникационного протокола в условиях реализации внешних программных угроз [97], которая базируется на результатах работы [26] и позволяет определить содержание и моменты времени передачи сообщений в тестовых способах реализации внешних программных угроз;
- 1.2) моделей функционирования ИТС в условиях реализации внутренних программных угроз [94-96], которые базируются на результатах работ [42, 44, 45, 52] и позволяют определить наборы действий оператора в тестовых способах реализации внутренних программных угроз.

Рис. 4. Технологическая схема процесса обеспечения конфликтной устойчивости программной реализации алгоритмов управления РЭА

Этап 2. Выявление программных угроз безопасности заданного образца РЭА, специфичных для его телекоммуникационных протоколов и программных человеко-машинных интерфейсов, с использованием:

- 2.1) алгоритма разработки множества тестовых способов реализации внешних программных угроз ИТС [93], который базируется на результатах работ [27, 30, 39, 48] и позволяет на основе п. 1.1 получить полное множество тестовых способов для оценки защищенности программной реализации алгоритмов управления ИТС от внешних программных угроз для доступной информации об используемой ИТС процедуре телекоммуникационного протокола;
- 2.2) алгоритмов разработки множества тестовых способов реализации внутренних программных угроз ИТС [94-96], которые базируются на результатах работ [39, 42, 44, 48, 49] и позволяют на основе п. 1.2 получить тестовые способы оценки функциональной пригодности, надежности, производительности, защищенности программной реализации алгоритмов управления ИТС от внутренних программных угроз.

Этап 3. Исследование конфликта ОТС, применяющих РЭА, с использованием:

- 3.1) моделей субпроцессов функционирования ИТС в конфликтных условиях [99, 100], которые базируются на результатах работ [45, 101] и позволяют на основе пп. 2.1, 2.2 получить вероятностно-временные

характеристики дискретно-событийных субпроцессов функционирования технического, общего и специального программного и информационного обеспечения, а также подсистемы защиты информации;

- 3.2) модели процесса функционирования ИТС [99], которая базируется на результатах работ [54, 60, 68] и позволяет на основе п. 3.1 оценить с учетом функциональной пригодности, надежности, производительности и защищенности программной реализации АЛУ этого средства следующие показатели: вероятность нахождения ИТС в работоспособном состоянии; вероятность внедрения ложной информации в ИТС с применением СПС; вероятность получения доступа к информации в ИТС с применением СПС; вероятность диверсионного использования ИТС с применением СПС; вероятность заражения других ИТС специальными программными средствами, находящимися в ИТС;
- 3.3) модели процесса распространения СПС в образуемых РЭА компьютерных сетях ОТС [102], которая базируется на результатах работ [9, 12, 28, 29] и позволяет оценить вероятность заражения каждого узлового ИТС сети несколькими экземплярами СПС одного или нескольких типов в различные моменты времени для случая, когда подсистемы защиты информации запоминают излеченные ими СПС, приобретая иммунитет к ним;
- 3.4) алгоритма аналитической оценки весовых коэффициентов элементов ОТС [103], который базируется на результатах работ [78, 82, 83] и позволяет оценить весовые коэффициенты элементов ОТС с учетом вклада каждого ИТС, входящего в РЭА;
- 3.5) моделей процессов, обеспечиваемых РЭА в конфликте ОТС [103-107], которые базируются на результатах работ [53, 55, 57, 61, 63, 66, 71-89] и позволяют на основе пп. 3.1-3.4 обеспечить разработку системы многоуровневых иерархических аналитических моделей процессов, обеспечиваемых РЭА в конфликте гетерогенных ОТС.

Этап 4. Определение программных угроз безопасности заданного образца РЭА, устранение которых обеспечит повышение или достижение требуемого уровня целевой эффективности его ОТС в конфликте с использованием алгоритма параметрического синтеза программной реализации алгоритмов управления РЭА. Этот алгоритм базируется на применении методов теории выбора и состоит в решении комбинированной задачи *O*-оптимального выбора на множестве эффективных альтернатив, полученном в результате решения задачи γ-эффективного выбора [91], согласно формуле (4) с использованием схемы, показанной на рис. 5.

Варианты набора исходных данных в данном алгоритме формируются путем комбинаторного сочетания варьируемых значений параметров защиты программной реализации алгоритмов управления ИТС заданного образца РЭА от ПВ, параметров времени подготовки этих ИТС к работе, параметров управления заданным образцом РЭА и параметров функционирования этого образца РЭА во всем диапазоне их допустимых значений.

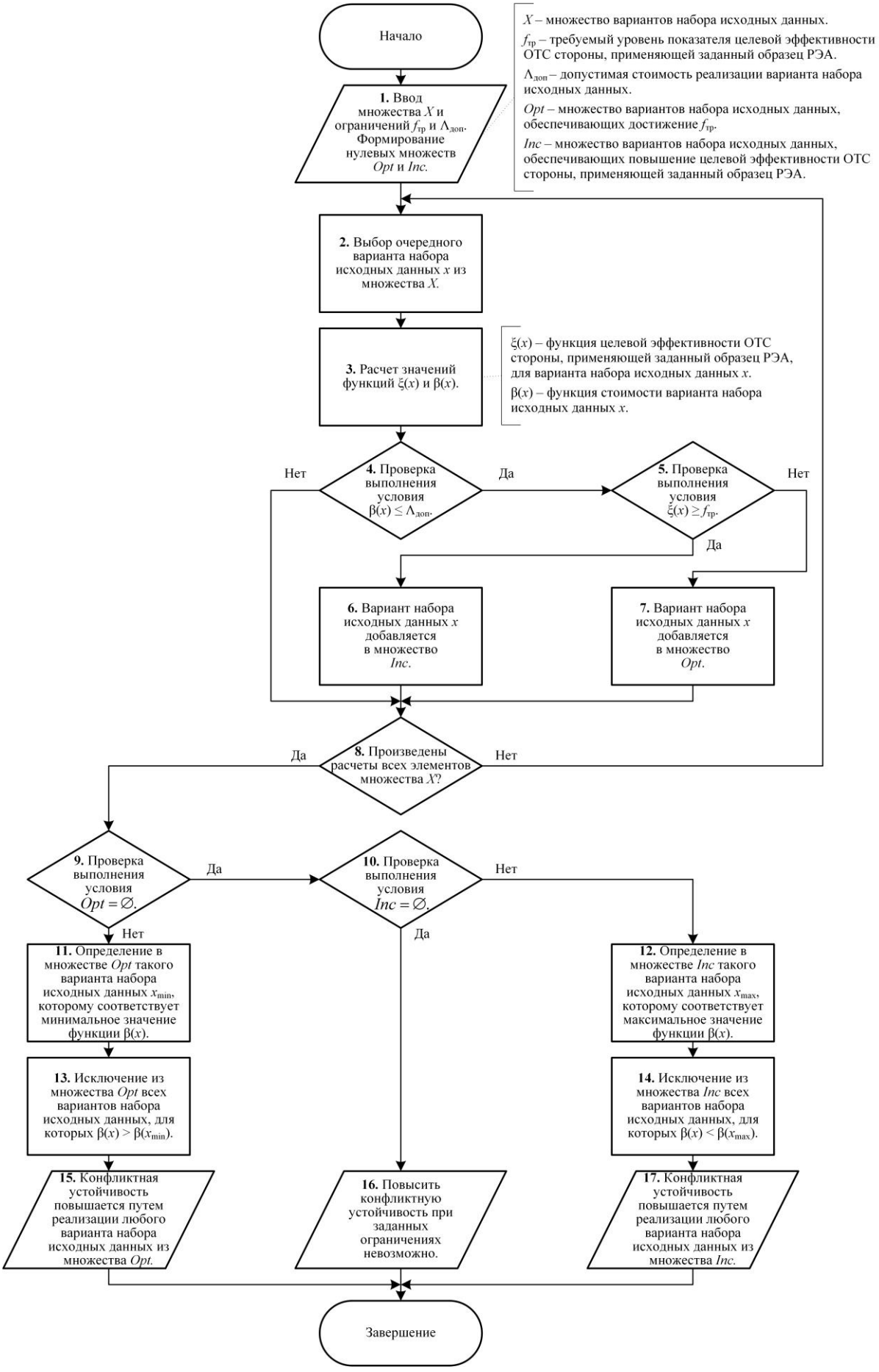

Рис. 5. Схема алгоритма параметрического синтеза программной реализации алгоритмов управления РЭА

По результатам применения этого алгоритма формируются рекомендации, содержащие численные значения параметров, которые должны быть достигнуты в ходе создания или модернизации заданного образца РЭА. Выполнение этих рекомендаций разработчиком образца РЭА позволит обеспечить необходимую конфликтную устойчивость программной реализации его АЛУ.

Применение метода сопряжено с выполнением значительного объема вычислений, производимых программными средствами, на которые даются ссылки в работах [93, 100, 103].

Пример применения метода

Задавая неизменными различные наборы варьируемых параметров и вводя дополнительные ограничения, метод трансформируется во множество методик обоснования численных значений параметров функциональной пригодности, производительности, надежности и защищенности программной реализации АЛУ радиоэлектронной аппаратуры ОТС. Рассмотрим пример применения методики обоснования требований к параметрам функциональной пригодности.

В качестве исходных данных в примере взят эпизод боя двух мотострелковых (мотопехотных) батальонов *А* и *Б* на равнинной местности. Продолжительность эпизода составляет 15 минут. В ходе эпизода элементы боевых порядков размещены на расстоянии до 5 км друг от друга. Огонь ведется без смены позиций. Состав, тактико-технические характеристики средств и информационные потоки батальонов одинаковые. Боевой порядок батальона состоит из командно-наблюдательного пункта (КНП) батальона, трех рот и отдельной позиции средства разведки. Элементами роты являются: КНП роты, девять средств огневого поражения из расчета по три в каждом из трех взводов. КНП взвода размещается на одном из его средств огневого поражения, а КНП батальонов и рот размещаются на позициях отдельных средств огневого поражения. Всеми элементами боевых порядков используются ИТС УКВ-радиосвязи, местоположение и информацию которых вскрывает средство разведки противника с вероятностью 0,9. Сектор стрельбы каждого средства огневого поражения охватывает весь боевой порядок противника. Вероятность попадания средства огневого поражения в цель в течение боевого эпизода равна 0,1.

В методике необходимо определить уровень функциональной пригодности программной реализации алгоритмов управления РЭА элементов боевого порядка одной из сторон конфликта, при котором ее целевая эффективность будет не менее требуемой. Целевую эффективность батальонов в боевом эпизоде будем оценивать по выигрышу в соотношении боевых потенциалов с применением моделей, описанных в [103-107]. Очевидно, что для одинаковых батальонов соотношение их боевых потенциалов равно нулю.

Пусть программная реализация АЛУ всех образцов РЭА батальона *А* полностью функционально пригодна, т.е. ее уровень равен 1. Тогда с применением предлагаемого метода можно получить зависимости боевого потенциала батальона *Б* от одинакового для всех образцов его РЭА уровня функциональной пригодности программной реализации АЛУ при различных уровнях информатизации Δ обоих батальонов. Эти зависимости показаны на рис. 6.

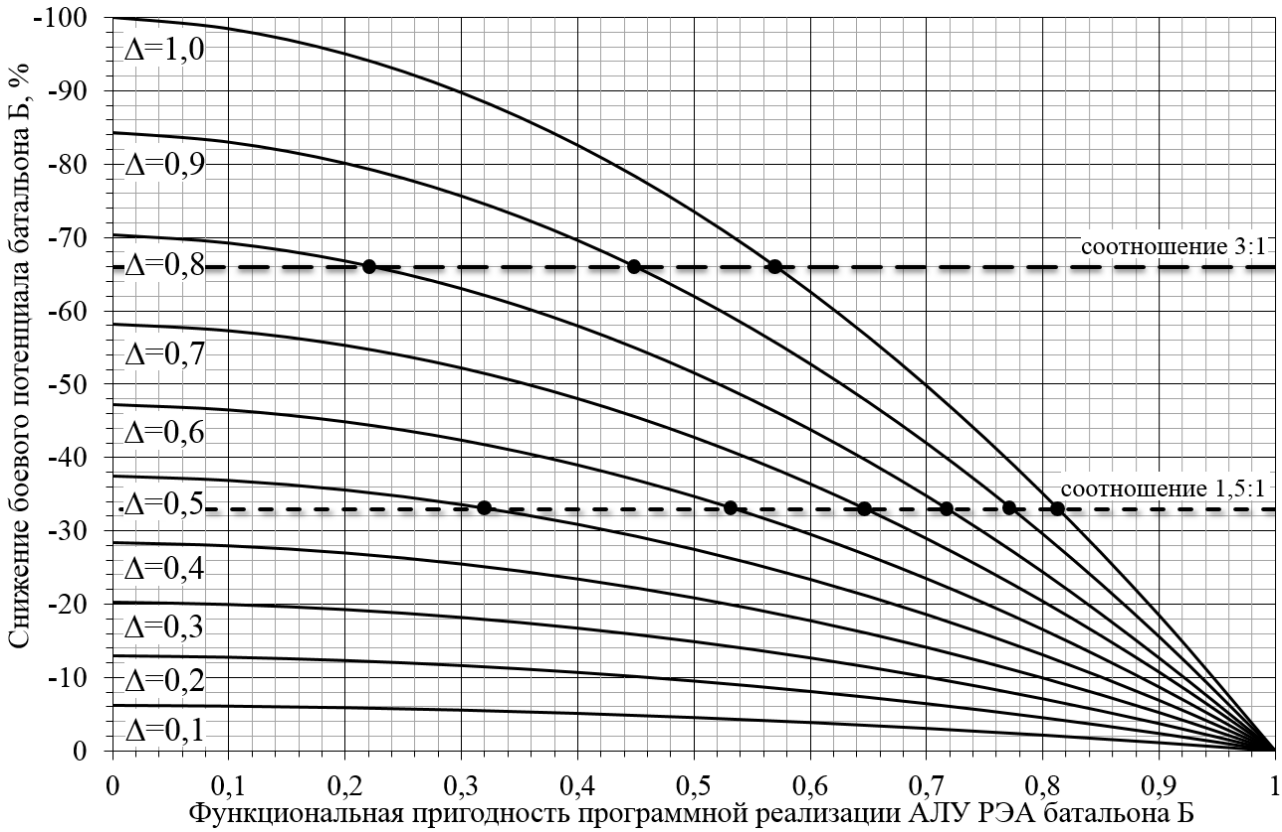

Рис. 6. Зависимости боевого потенциала батальона *Б* от уровня функциональной пригодности программной реализации АЛУ его РЭА

При планировании вооруженных конфликтов широко используются эмпирически устанавливаемые критерии соотношения боевых потенциалов противоборствующих сторон. Например, общеизвестно, что атаковать укрепленные позиции целесообразно при соотношении боевых потенциалов не менее «3:1» (или «1:0,33»), а атаковать не укрепившегося на местности противника целесообразно при соотношении не менее «1,5:1» (или «1:0,66»). С учетом этого анализ зависимостей на рис. 6 позволяет сделать следующие выводы.

Во-первых, в рассматриваемом боевом эпизоде существенными являются уровни информатизации батальонов, равные 0,5 и выше.

Во-вторых, при обороне батальона *Б* на укрепленных позициях функциональная пригодность программной реализации АЛУ его РЭА должна быть при Δ=0,8 не менее 0,22, при Δ=0,9 не менее 0,45 и при Δ=1 не менее 0,65.

В-третьих, при обороне батальоном *Б* на неукрепленных позициях функциональная пригодность программной реализации АЛУ его РЭА должна быть при Δ=0,5 не менее 0,32, при Δ=0,6 не менее 0,53, при Δ=0,7 не менее 0,65, при Δ=0,8 не менее 0,72, при Δ=0,9 не менее 0,77 и при Δ=1 не менее 0,81.

Поскольку воинское формирование должно применяться в различных условиях боя, то критерии функциональной пригодности программной реализации алгоритмов управления РЭА его элементов боевого порядка необходимо выбрать для наихудших условий, т.е. для обороны на неукрепленных позициях.

Исходные данные рассмотренного примера значительно упрощены, поскольку имеют исключительно ознакомительный характер. На практике в качестве исходных данных могут использоваться реальные вооруженные конфлик-

ты, которые характеризуются высокой динамикой и существенной разнородностью используемых сил и средств как по выполняемым функциям и уровням информатизации, так и по функциональной пригодности программной реализации АЛУ не только отдельных образцов РЭА, но и входящих в ее состав отдельных образцов ИТС.

Для развития данного метода требуется решение следующих задач:

1) автоматического синтеза тестовых сценариев реализации программных угроз РЭА в конфликте ОТС;
2) оптимизации целераспределения и размещения элементов гетерогенных ОТС в конфликте;
3) анализа динамики целевой эффективности ОТС в конфликте при различных траекториях изменения местоположения ее элементов.

Первую задачу целесообразно решать известными методами комбинаторного анализа и динамического программирования и методами теории тестирования, а вторую и третью с использованием комбинации известных методов теории искусственного интеллекта и теории игр.

Заключение

В работе предложен *метод упреждающего парирования программных угроз* безопасности радиоэлектронной аппаратуры пространственно распределенных гетерогенных организационно-технических систем. Он состоит в выявлении внешних и внутренних программных угроз, специфичных для телекоммуникационных протоколов и программных человеко-машинных интерфейсов заданного образца радиоэлектронной аппаратуры, и определении тех из них, устранение которых обеспечит повышение или достижение требуемого уровня целевой эффективности его организационно-технической системы в конфликте.

Метод впервые позволяет получить ответы на три следующих вопроса.

1. Как качество программной реализации алгоритмов управления заданным образцом радиоэлектронной аппаратуры влияет на целевую эффективность его организационно-технической системы в конфликте?

2. Какими должны быть значения параметров программной реализации алгоритмов управления заданным образцом радиоэлектронной аппаратуры, чтобы его система в конфликтных условиях имела целевую эффективность не ниже требуемой, и достижимо ли в принципе требуемое значение целевой эффективности для имеющихся исходных данных?

3. Какие программные угрозы безопасности заданного образца радиоэлектронной аппаратуры нужно устранить для достижения требуемого значения или повышения целевой эффективности организационно-технической системы, в состав которой этот образец входит?

Предлагаемый метод отличается следующей новизной.

Во-первых, в логико-алгебраической модели информационного взаимодействия информационно-технических средств в рамках заданной процедуры телекоммуникационного протокола при реализации внешних программных угроз *в отличие от* модели функционирования одного информационно-технического средства в процессе его взаимодействия с другими информацион-

но-техническими средствами, изложенной в [26], *введено* дискретно-событийное представление процесса одновременного информационного взаимодействия нескольких информационно-технических средств. В нем каждое состояние соответствует последовательности процессов от формирования и передачи одного сообщения с актуальным для заданной процедуры телекоммуникационного протокола гранулярным информационным элементом до приема этого сообщения. Переход между состояниями соответствует процессу функционирования общего для этих состояний информационно-технического средства с момента отправки или получения сообщения до момента отправки этим средством другого сообщения без промежуточных входящих сообщений (прямой переход, легитимный) или через одно входящее сообщение (опосредованный переход, соответствующий потенциальной внешней программной угрозе).

Во-вторых, в графоаналитических моделях функционирования информационно-технического средства в условиях реализации внутренних программных угроз, рассматривающих это средство с позиции «черного ящика», в *отличие от* моделей, изложенных в [42, 44, 45, 52], *введены*:

1) граф управляющей структуры программного человеко-машинного интерфейса информационно-технического средства, описывающий причинно-следственные связи действий, доступных человеку-оператору, и реакций на эти действия элементов интерфейса;
2) деревья α-уровней, описывающие причинно-следственные связи задач, выполняемых информационно-техническими средствами.

В-третьих, в комбинаторном алгоритме разработки множества тестовых способов реализации внешних программных угроз безопасности информационно-технического средства, функционирующего в рамках заданной процедуры телекоммуникационного протокола, *в отличие от* алгоритмов, изложенных в [27, 30, 39, 48], в тестовых способах *введены* факторы своевременности и прецизионности тестовых сообщений, которые при комплексном сочетании с известными факторами кратности и правильности позволяют сформировать полное множество тестовых способов реализации внешних программных угроз безопасности информационно-технического средства для доступной информации об алгоритмах управления им.

В-четвертых, в комбинаторных алгоритмах разработки множества тестовых способов реализации внутренних программных угроз безопасности информационно-технического средства, рассматривающих это средство с позиции «черного ящика», *в отличие от* алгоритмов, изложенных в [39, 42, 44, 48, 49], *дополнительно производится* проверка корректности:

1) потоков управления и данных в программном человеко-машинном интерфейсе;
2) последовательностей выполнения задач в информационно-техническом средстве согласно их причинно-следственным связям.

В-пятых, в аналитических моделях субпроцессов функционирования информационно-технического средства в конфликтных условиях *в отличие от* моделей, изложенных в [45, 101], дополнительно *введены*:

1) дискретно-событийная модель информационного конфликта специального программного средства, реализующего внешние программные угрозы безопасности радиоэлектронной аппаратуры, и подсистемы защиты информации информационно-технического средства;
2) состояния в дискретно-событийной модели функционирования технического обеспечения: «уничтожено», характерное для антагонистического конфликта, и «функционирует с нулевой производительностью», возникающее при поражении электромагнитным излучением элементной базы радиоэлектронной аппаратуры с обратимым эффектом.

В-шестых, в аналитической модели процесса функционирования информационно-технического средства *в отличие от* моделей, изложенных в [54, 60, 68], это средство *описывается как единый комплекс* одновременно реализуемых дискретно-событийных субпроцессов функционирования технического обеспечения, общего программного и информационного обеспечения, подсистемы защиты информации, а также специального программного и информационного обеспечения информационных, расчетных, телекоммуникационных задач и задач управления, которые координируются диспетчером в виде системы массового обслуживания.

В-седьмых, в аналитической модели процесса распространения специальных программных средств в образуемых радиоэлектронной аппаратурой компьютерных сетях организационно-технических систем *в отличие от* моделей, изложенных в [9, 12, 28, 29], *одновременно учитывается* сетевая архитектура, поведенческие характеристики специальных программных средств и подсистем защиты информации каждого узла сети, а также возможности заражения множества узлов сети различными типами специальных программных средств в любой момент времени.

В-восьмых, в алгоритме оценки весовых коэффициентов элементов организационно-технической системы *в отличие от* алгоритмов, изложенных в [78, 82, 83], *исключена* необходимость проведения экспертных оценок и натурных экспериментов за счет последовательного вычисления значений показателя целевой эффективности такой системы без каждого из ее элементов и вычислении весового коэффициента каждого элемента по величине ущерба, наносимого целевой эффективности системы его исключением.

В-девятых, в моделях процессов, обеспечиваемых радиоэлектронной аппаратурой в конфликте организационно-технических систем, *в отличие от* моделей, изложенных в [53, 55, 57, 61, 63, 66, 71-89], *введены*:

1) когнитивный фактор, влияющий на целевую эффективность организационно-технических систем, применяющих радиоэлектронную аппаратуру в конфликтных условиях. Этот фактор характеризует информацию в OODA-циклах организационно-технических систем (циклах «наблюдение-ориентация-решение-действие»). Вводимый фактор совместно с известными энергетическим фактором (средства деструктивного воздействия и защиты от них), информационно-телекоммуникационным фактором (каналы связи и разведки), ресурсным фактором и психологическим фактором (психическая деятель-

ность людей, уровень их подготовки, опыта и слаженности работы) используется в аналитических выражениях, описывающих процессы функционирования элементов организационно-технических систем на уровне полумарковских моделей их информационно-технических средств, плотность распределения вероятности времени переходов в которых зависит от взаимного влияния конфликтующих организационно-технических систем при статичном размещении на местности позиций их элементов в течение эпизода конфликта;

2) графоаналитическая модель позиционной динамики элементов организационно-технических систем в конфликте в заданном районе, отражающая в каждый момент времени интегральный результат конфликта во всех альтернативных последовательностях его эпизодов с учетом вероятности реализации этих последовательностей. В модели динамика показателей целевой эффективности организационно-технических систем в соседних районах агрегируется до заданного уровня с учетом иерархической вложенности организационно-технических систем.

Предлагаемый метод может быть полезен при модернизации существующих и создании перспективных образцов конфликтно-устойчивой радиоэлектронной аппаратуры.

Литература

1. Бойко А. А., Балыбин В. А., Донсков Ю. Е. О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства // Военная Мысль. 2013. № 9. С. 28-32.

2. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М. Стандартинформ, 2007. – 10 с.

3. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

4. Климов С. М. Методы и модели противодействия компьютерным атакам. – Люберцы: Каталист, 2008. – 316 с.

5. ГОСТ Р ИСО/МЭК 25010-2015 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения. – М. Стандартинформ, 2015. – 36 с.

6. Петухов Г. Б. Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, цели. – М.: МО СССР, 1989. – 660 с.

7. Антушев Г. С. Методы параметрического синтеза сложных технических систем. – М.: Наука, 1989. – 88 с.

8. Раскин Л. Г. Анализ сложных систем и элементы теории оптимального управления. – М.: Сов. Радио, 1976. – 344 с.

9. Бабанин Д. В., Далингер Я. М., Бурков С. М. Математические модели распространения вирусов в компьютерных сетях различной структуры // Информатика и системы управления. 2012. № 3 (33). С. 25-33.

10. Антонов С. Г., Климов С. М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Т. 17. № 1 (60). С. 32-39.

11. Костогрызов А. И. Резников Г. Я. Моделирование процессов опасного воздействия на защищаемую информационную систему // Информационные технологии в проектировании и производстве. 2004. № 2. С. 17-27.

12. Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. 2007. № 4. С. 208-224.

13. Коцыняк М. А., Осадчий А. И., Коцыняк М. М., Лаута О. С., Дементьев В. Е., Васюков Д. Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. – СПб.: ЛО ЦНИИС, 2015. – 126 с.

14. Домбровский А. Ф., Ломако А. Г., Матвеев С. А., Петриенко А. С. Метод восстановления неизвестных протоколов передачи данных на основе теории взаимодействующих последовательных процессов Ч. Хоара // I International Conference «The 2017 Symposium on Cybersecurity of the Digital Economy – CDE'17». С. 150-154.

15. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. – СПб.: Наукоемкие технологии, 2018. – 122 с.

16. Белоножкин В. И., Остапенко Г. А. Информационные аспекты противодействия терроризму. – М.: Горячая линия – Телеком, 2009. – 112 с.

17. Толстых Н. Н., Остапенко А. Г., Толстых И. О., Ахромеев М. В. Распространение вирусов в кластеризованной сети мобильной связи // Информация и безопасность. 2008. № 3. С. 441-444.

18. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия // Труды ИСА РАН. 2009. Т. 41. С. 104-146.

19. Зорин Э. Ф., Рыжов Б. С., Володина Н. И. Оценка информационной безопасности средств информатизации автоматизированных систем военного назначения в условиях информационно-технических воздействий // Информационные войны. 2018. № 1 (45) С. 84-87.

20. Волков Д. В., Саенко И. Б., Старков А. М., Султанбеков А. Т. Оценка устойчивости сети передачи данных в условиях деструктивных воздействий // Известия Тульского государственного университета. Технические науки. 2018. № 12. С. 358-363.

21. Семенов С. С., Гусев А. П., Барботько Н. В. Оценка информационно-боевого потенциала сторон в техносферных конфликтах // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 6. С. 10-21.

22. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Информационные системы и технологии. 2011. № 1. С. 80-85.

23. Иванкин М. П. Толстых Н. Н., Савинков А. Ю., Свердел В. Ф. К вопросу оценки эффективности функционирования систем программно-

определяемого радио в условиях информационного конфликта // Теория и техника радиосвязи. 2018. № 4. С. 14-18.

24. Хоар Ч. Взаимодействующие последовательные процессы. – М.: Мир, 1989. – 264 с.

25. Текунов В. В., Язов Ю. К. Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри-Маркова // Информация и безопасность. 2018. Т. 21. № 1. С. 38-47.

26. Charrton-Bost B., Mattern F., Tel G. Synchronous, Asynchronous, and Casually Ordered Communication // Distributed Comput. 1996. Vol. 9. pp. 173-191.

27. Clarke E. M., Grumberg O., Peled D. Model Checking. – N. Y.: MIT Press, 1999. – 314 p.

28. Gan C., Yang X., Liu W., Zhu Q. A propagation model of computer virus with nonlinear vaccination probability // Communications in Nonlinear Science and Numerical Simulation. 2014. vol. 19. no. 1. pp. 92-100.

29. Mishra B. K., Jha N. SEIQRS model for the transmission of malicious objects in computer network // Applied Mathematical Modelling. 2010. Vol. 34. No. 3. pp.710-715.

30. Hayhurst K. J., Veerhusen D. S., Chilenski J. J., Rierson L. K. A Practical Tutorial on Modified Condition / Decision Coverage. – NASA, 2001. – 85 p.

31. Перегудов М. А., Бойко А. А. Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7-15.

32. Перегудов М. А., Бойко А. А. Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75-81.

33. Перегудов М. А., Бойко А. А. Модель процедуры управления питанием сети пакетной радиосвязи // Телекоммуникации. 2015. № 9. С. 13-18.

34. Перегудов М. А., Бойко А. А. Оценка защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA // Информационные технологии. 2015. Т. 21. № 7. С. 527-534.

35. Перегудов М. А., Семченко И. А. Оценка эффективности случайного множественного доступа к среде типа ALOHA при голосовых соединениях, передаче служебных команд, текстовых сообщений и мультимедийных файлов в условиях деструктивных воздействий // Труды СПИИРАН. 2019. Т. 18. № 4. С. 887-911.

36.Перегудов М. А., Стешковой А. С., Бойко А. А. Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA // Труды СПИИРАН. 2018. № 4. С. 92-114.

37. Жуматий В. П., Будников С. А., Паршин Н. В. Угрозы программно-математического воздействия. – Воронеж: ЦПКС ТЗИ, 2010. – 230 с.

38. Баранов С. Н., Домарацкий А. Н., Ласточкин Н. К., Морозов В. П. Процесс разработки программных изделий. – М.: Наука, Физматлит, 2000. – 176 с.

39. Beizer B. Black-Box Testing. – New York: Wiley, 1995. – 324 p.

40. Генельт А. Е. Управление качеством разработки программного обеспечения: – СПб: ИТМО, 2007. – 187 с.

41. Грошев С. Г. Применение технологии UniTesK для тестирования систем с различной конфигурацией активных потоков управления // Труды Института системного программирования. 2006. Т. 9. С. 67-82.

42. Канер С., Фолк Дж., Нгуен Е. Тестирование программного обеспечения. – Киев: Издательство DiaSoft, 2001. – 554 с.

43. Кулямин В. В. Методы верификации программного обеспечения. – М.: ИСП РАН, 2008. – 111 с.

44. Липаев В. В. Тестирование программ. – М.: Радио и связь, 1986. – 296 с.

45. Половко А. М., Гуров С. В. Основы теории надежности. – СПб.: БХВ-Петербург, 2006. – 704 с.

46. Тейер Т. Липов М., Нельсон Э. Надежность программного обеспечения. – М.: Мир, 1981. – 323 с.

47. Карповский Е. Я., Чижов С. А. Надежность программной продукции. – Киев: Техника, 1990. – 160 с.

48. Myers G. J. The Art of Software Testing. – New Jersey: John Wiley & Sons, 2004. – 255 p.

49. Porteuos M., Kirakowski J., Cutts D. Software usability measurement inventory User Handbook. – Cork: Human Factors Research Group, University College, 1993. – 54 p.

50. ГОСТ Р ИСО/МЭК 25041-2014 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения. Руководство по оценке для разработчиков, приобретателей и независимых оценщиков. – М. Стандартинформ, 2014. – 43 с.

51. ГОСТ Р ИСО/МЭК 9126-93 Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. – М.: ГОССТАНДАРТ России, 1993. – 12 с.

52. ISO/IEC/IEEE 29119-4: Software and Systems Engineering. Software Testing. Part 4: Test Techniques. – ISO/IEC JTC 1/ SC 7. – 139 p.

53. Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. – М.: Советское радио, 1968. – 448 с.

54. Владимиров В. И., Владимиров И. В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). – Воронеж: ВАИУ, 2008. – 231 с.

55. Владимиров В. И., Лихачев В. П., Шляхин В. М. Антагонистический конфликт радиоэлектронных систем. Методы и математические модели. – М.: Радиотехника, 2004. – 384 с.

56. Владимиров В. И., Стучинский В. И. Выбор системы показателей информационного превосходства в операциях в условиях двухсторонней радиоэлектронной борьбы // Военная Мысль. 2016. № 10. С. 33-39.

57. Дружинин В. В., Конторов Д. С., Конторов М. Д. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.

58. Петров А. В., Яковлев А. А. Анализ и синтез радиотехнических комплексов / Под ред. В.Е. Дулевича. – М.: Радио и связь, 1984. – 248 с.

59. Козлов С. В., Карпухин В. И., Лазаренков С. М. Модели конфликта авиационных систем радиоэлектронной борьбы и противовоздушной обороны. – Воронеж: ВУНЦ ВВС «ВВА», 2013. – 468 с.

60. Будников С. А., Гревцев А. И., Иванцов А. В., Кильдюшевский В. М., Козирацкий А. Ю., Козирацкий Ю. Л., Кущев С. С., Лысиков В. Ф., Паринов М. Л., Прохоров Д. В. Модели информационного конфликта средств поиска и обнаружения. – М.: Радиотехника, 2013. – 232 с.

61. Губарев В. А., Крутских П. П. Концептуальная модель конфликта в информационной борьбе // Радиотехника. 1998. № 6. С. 29-31.

62. Кузнецов В. И. Радиосвязь в условиях радиоэлектронной борьбы. – Воронеж: ВНИИС. 2002. – 403 с.

63. Поддубный В. Н., Агафонов А. А., Ложкин К. Ю. Методология и результаты синтеза и оценки эффективности преднамеренных помех приемникам дискретных сигналов // Радиотехника и электроника. 2003. Т. 48. № 8. С. 956-962.

64. Мочалов С. А. Автоматизированный синтез многофункциональной интегрированной радиоэлектронной системы. Методология исследования авиационных комплексов ВМФ. – М.: Радиотехника, 2014. – 240 с.

65. Перунов Ю. М., Фомичев К. И., Юдин Л. М. Радиоэлектронное подавление информационных каналов систем управления оружием. – М.: Радиотехника, 2003. – 416 с.

66. Агафонов А. А., Артюх С. Н., Афанасьев В. И., Афанасьева Е. М., Бостынец И. П., Быков В. В., Донцов А. А., Ермаков А. И., Калинков А. К., Каунов А. Е., Кирсанов Э. А., Лаптев И. В., Ложкин К. Ю., Марек Я. Л., Миронов В. А., Нечаев С. С., Новиков И. И., Овчаренко Л. А., Огреб С. М., Поддубный В. Н., Понькин В. А., Радзиевский В. Г., Разиньков С. Н., Романов А. Д., Рыжов А. В., Сирота А. А., Соловьев В. В., Сорокин Ю. А., Сухоруков Ю. С., Телков А. Ю., Уфаев В. А., Харченко Т. В., Юхно П. М., Яньшин С. Н. Современная радиоэлектронная борьба. Вопросы методологии. – М.: Радиотехника, 2006. – 424 с.

67. Цветков А. Г. Принципы количественной оценки эффективности радиоэлектронных средств. – М.: Сов. Радио, 1971. – 200 с.

68. Чикин М. Г. Особенности использования аппарата полумарковских процессов для моделирования направлений радиосвязи в интересах оценки эффективности радиоподавления // Радиотехника. 2005. № 9. С. 35-39.

69. Астапенко Ю. А., Вайпан С. Н., Вакуленко А. А., Вакуленко Н. Н., Верба Б. С., Грибков Р. А., Гузенко О. Б., Дод В. Н., Зайцев А. Г., Иванов А. Н., Ионкин А. А., Король О. В., Кузьмин Г. В., Лясковский В. Л., Марухленко А. С., Неплюев О. Н., Приступюк И. А., Проскурин В. И., Рюмшин А. Р., Самушкин А. Н., Сенчаков Г. В., Турко Н. И., Шевчук В. И., Шевчук Д. В., Ягольников С. В. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза. – М.: Радиотехника, 2015. – 312 с.

70. Adamy D. L. EW 104: Electronic Warfare against a New Generation of Threats. – Boston-London: Artech House, 2015. – 491 p.

71. Новиков Д. А. Иерархические модели военных действий // Управление большими системами. 2012. № 37. С. 25-61.

72. Алексеев О. Г., Анисимов В. Г., Анисимов Е. Г. Модели распределения средств поражения в динамике боя. – М.: МО СССР, 1989. – 110 с.

73. Арбузов И. В., Болховитинов О. В., Волочаев О. В., Вольнов И. И., Гостев А. В., Мышкин Л. В., Хабиров Р. Н., Шеховцов В. Л. Боевые авиационные комплексы и их эффективность. – М.: ВВИА им. проф. Н.Е. Жуковского, 2008. – 224 с.

74. Борисов В. В., Сысков В. В. Мультиагентное моделирование сложных организационно-технических систем в условиях противоборства // Информационные технологии. 2012. № 4. С. 7-14.

75. Буравлев А. И., Горшков П. С. К вопросу о построении агрегированной модели противоборства группировок войск // Вооружение и экономика. 2017. № 5 (42). С. 35-48.

76. Вайнер А. Я. Тактические расчеты. – М.: Воениздат, 1982. – 176 с.

77. Гирин А. В. Усовершенствованная методика определения боевых возможностей общевойсковой группировки войск // Военная Мысль. 2012. № 10. С. 26-30.

78. Захаров Л. В., Богданов С. А. О выработке единых подходов к оценке боевых потенциалов // Военная Мысль. 1992. № 8-9. С. 42-49.

79. Меркулов С. Н., Сухоруков Ю. С., Донсков Ю. Е. Проблемы автоматизации интеллектуальной поддержки принятия решений общевойсковыми командирами в тактическом звене // Военная Мысль. 2009. № 9. С.43-53.

80. Митюков Н. В. Имитационное моделирование в военной истории. – М.: ЛЕНАНД, 2018. – 280 с.

81. Поленин В. И., Сущенков Д. А. Разработка модели вооруженного противоборства боевых систем тактического уровня с нанесением ударов непосредственно по боевой системе противника и отражением ударов противника по своей боевой системе // Национальная ассоциация ученых. 2015. № 8 (17). С. 167-171.

82. Сосюра О. В. Расчет обобщенных показателей боевых возможностей войск в операциях (боевых действиях) с учетом эффективности управления ими (потенциально-долевой метод). – М.: Военная Мысль, 1997. – 142 с.

83. Тараканов К. В. Математика и вооруженная борьба. – М.: Воениздат, 1974. – 240 с.

84. Ткаченко П. Н., Куцев Л. Н., Мещеряков Г. А., Чавкин А. М., Чебыкин А. Д. Математические модели боевых действий. – М.: Советское радио, 1969. – 240 с.

85. Фендриков Н. М., Яковлев В. И. Методы расчетов боевой эффективности вооружения. – М.: Военное издательство, 1971. – 224 с.

86. Черноскутов А. И., Ситкевич А. В., Тришкин В. С. Рациональный способ уничтожения разнородных группировок // Военная Мысль. 2018. № 1. С. 63-67.

87. Чуев Ю. В. Исследование операций в военном деле. – М.: Воениздат, 1970. – 256 с.

88. Chowdhury S. M., Kovenock D., Sheremeta R. M. An Experimental Investigation of Colonel Blotto Games // CESifo Working Paper. 2009. № 2688. 36p.

89. Washburn A., Kress M. Combat Modeling. – London: Springer, 2009. – 281 p.

90. Kress, M. Caulkins J. P., Feichtinger G., Grass D., Seidl A. Lanchester model for three-way combat // European Journal of Operational Research. 2018. № 1 (264). pp. 46-54.

91. Калинин В. Н., Резников Б. А., Варакин Е. И. Теория систем и оптимального управления. Часть 2. Понятия, модели, методы и алгоритмы оптимального выбора. – М.: МО СССР, 1987. – 589 с.

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

93. Бойко А. А., Обущенко Е. Ю., Щеглов А. В. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. Серия: системный анализ и информационные технологии. 2017. № 2. С. 33-45.

94. Бойко А. А., Храмов В. Ю. Методика оценки правильности и устойчивости к ошибкам специального программного обеспечения автоматизированных систем военного назначения // Вестник Воронежского государственного университета. Серия: системный анализ и информационные технологии. 2007. № 1. С. 106-115.

95. Бойко А. А., Храмов В. Ю. Методика оценки пригодности специального программного обеспечения автоматизированных систем и средств управления // Вестник Воронежского военного института. 2007. № 1 (6). С. 218-225.

96. Бойко А. А., Храмов В. Ю. Формирование тестовых последовательностей выполнения информационно-расчетных задач при оценке частных показателей качества специального программного обеспечения // Сборник трудов Всероссийской научно-технической конференции адъюнктов, аспирантов, соискателей и молодых специалистов. – Воронеж: ФГНИИЦ РЭБ ОЭСЗ Минобороны России, 2008. – С. 295-301.

97. Бойко А. А., Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84-92.

98. Бойко А. А. Способ оценки уровня информатизации образцов вооружения // Системы управления, связи и безопасности. 2019. № 1. С. 264-275.

99. Бойко А. А. Способ стратифицированного аналитического описания процесса функционирования информационно-технических средств // Информационные технологии. 2015. № 1. С. 35-42.

100. Бойко А. А., Будников С. А. Модель информационного конфликта специального программного средства и подсистемы защиты информации информационно-технического средства // Радиотехника. 2015. № 4. С. 136-141.

101. Клейнрок Л. Вычислительные системы с очередями. – М.: Мир, 1979. – 600 с.

102. Бойко А. А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. № 5. С. 196-211.

103. Бойко А. А., Дегтярев И. С. Метод оценки весовых коэффициентов элементов организационно-технических систем // Системы управления, связи и безопасности. 2018. № 2. С. 245-266.

104. Бойко А. А. Способ аналитического моделирования боевых действий // Системы управления, связи и безопасности. 2019. № 2. С. 1-27. DOI: 10.24411/2410-9916-2019-10201.

105. Бойко А. А. О защищенности информации воинских формирований в современном вооруженном противоборстве // Военная Мысль. 2016. № 4. С. 38-51.

106. Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. № 7. С. 5-10.

107. Бойко А. А. Метод разработки иерархических многоуровневых моделей для аналитической оценки соотношения сил воинских формирований // Военная Мысль. 2019. № 7. С. 104-113.

References

1. Boyko A. A., Balybin V. A., Donskov Yu. E. O terminologii v oblasti radioelektronnoj bor'by v usloviyah sovremennogo informacionnogo protivoborstva [About the Terminology in the Field of Electronic Warfare in the Modern Information Warfare]. *Military Thought*, 2013, no. 9, pp. 28-32 (in Russian).

2. State Standard R 51275-2006 *Protection of Information. Object of Informatization. Factors Influencing the Information. General*. Moscow, Standartov Publ., 2007. 10 p. (in Russian).

3. Grinyaev S. N. *Intellektual'noe protivodejstvie informacionnomu oruzhiyu* [Intelligent Counter Information Weapons]. Moscow, SINTEG Publ., 1999. 232 p. (in Russian).

4. Klimov S. M. *Metody i modeli protivodejstviya komp'yuternym atakam* [Methods and Models of Countering Computer Attacks]. Lyubercy, Katalist Publ., 2008. 316 p. (in Russian).

5. State Standard R ISO/IEC 25010-2015 *Informacionnye tekhnologii. Sistemnaya i programmnaya inzheneriya. Trebovaniya i ocenka kachestva sistem i programmnogo obespecheniya* [Information technology. Systems and software

engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models]. Moscow, Standartov Publ., 2015. 36 p. (in Russian).

6. Petuhov G. B. *Osnovy teorii effektivnosti celenapravlennyh processov. CHast' 1. Metodologiya, metody, celi* [Fundamentals of the Theory of Efficiency of Purposeful Processes. Part 1. Methodology, Methods, Objectives]. Moscow, Ministry of Defense of the USSR, 1989. 660 p. (in Russian).

7. Antushev G. S. *Metody parametricheskogo sinteza slozhnyh tekhnicheskih sistem* [Methods of Parametric Synthesis of Complex Technical Systems]. Moscow, Nauka Publ., 1989. 88 p. (in Russian).

8. Raskin L. G. *Analiz slozhnyh sistem i elementy teorii optimal'nogo upravleniya* [Analysis of Complex Systems and Elements of Optimal Control Theory]. Moscow, Soviet Radio Publ., 1976. 344 p. (in Russian).

9. Babanin D. V., Dalinger Ya. M., Burkov S. M. Matematicheskie modeli rasprostraneniya virusov v komp'yuternyh setyah razlichnoj struktur [Mathematical Models of Virus Propagation in Computer Networks with Different Structures]. *Information Science and Control Systems*, 2012, no. 3 (33), pp. 25-33 (in Russian).

10. Antonov S. G., Klimov S. M. Metodika ocenki riskov narusheniya ustojchivosti funkcionirovaniya programmno-apparatnyh kompleksov v usloviyah informacionno-tekhnicheskih vozdejstvij [The Methods of Risk Assessment of the Stability of the Functioning of Software-hardware Systems in Terms of Information-Technical Impacts]. *Reliability*, 2017, vol. 17, no. 1 (60), pp. 32-39 (in Russian).

11. Kostogryzov A. I. Reznikov G. Ya. Modelirovanie processov opasnogo vozdejstviya na zashchishchaemuyu informacionnuyu sistemu [Modeling of Processes of Dangerous Influence on the Protected Information System]. *Information Technologies in Design and Production*, 2004, no. 2, pp. 17-27 (in Russian).

12. Kotenko I. V., Voroncov V. V. Analiticheskie Modeli rasprostraneniya setevyh chervej [Analytical Models of Network Worms Distribution]. *SPIIRAS Proceedings*, 2007, no. 4, pp. 208-224 (in Russian).

13. Kocynyak M. A., Osadchij A. I., Kocynyak M. M., Lauta O. S., Dement'ev V. E., Vasyukov D. Yu. *Obespechenie ustojchivosti informacionno-telekommunikacionnyh sistem v usloviyah informacionnogo protivoborstva* [Ensuring the Stability of Information and Telecommunication Systems in the Information Confrontation]. Saint-Petersburg, LO TsNIIS Publ., 2015. 126 p. (in Russian).

14. Dombrovskij A. F., Lomako A. G., Matveev S. A., Petrienko A. S. Metod vosstanovleniya neizvestnyh protokolov peredachi dannyh na osnove teorii vzaimodejstvuyushchih posledovatel'nyh processov CH. Hoara [The Method of Recovery of Unknown Data Transfer Protocols Based on the Theory of Interacting Sequential Processes by C. Hoare]. *I International Conference «The 2017 Symposium on Cybersecurity of the Digital Economy – CDE'17»*, pp. 150-154 (in Russian).

15. Makarenko S. I. Audit bezopasnosti kriticheskoj infrastruktury special'nymi informacionnymi vozdejstviyami [Security Audit of Critical Infrastructure by Special Information Impacts]. Saint-Petersburg, Naukoemkie tekhnologii Publ., 2018. 122 p. (in Russian).

16. Belonozhkin V. I., Ostapenko G. A. *Informacionnye aspekty protivodejstviya terrorizmu* [Information Aspects of Counter-Terrorism]. Moscow, Goryachaya liniya – Telekom Publ., 2009. 112 p. (in Russian).

17. Tolstyh N. N., Ostapenko A. G., Tolstyh I. O., Ahromeev M. V. Rasprostranenie virusov v klasterizovannoj seti mobil'noj svyazi [Virus Propagation in a Clustered Mobile Network]. *Information and Security*, 2008, no. 3, pp. 441-444 (in Russian).

18. Petrenko S. A. Metody informacionno-tekhnicheskogo vozdejstviya na kibersistemy i vozmozhnye sposoby protivodejstviya [Methods of Information-Technical Impacts on Cybersystems and Possible Ways of Counteraction]. *Proceedings of the Institute of System Analysis of the RAS*, 2009, vol. 41, pp. 104-146. (in Russian).

19. Zorin E. F., Ryzhov B. S., Volodina N. I. Ocenka informacionnoj bezopasnosti sredstv informatizacii avtomatizirovannyh sistem voennogo naznacheniya v usloviyah informacionno-tekhnicheskih vozdejstvij [Assessment of Information Security of Informatization Means of Automated Systems for Military Purposes in the Conditions of Information-Technical Impacts]. *Informsionatnye voiny*, 2018, no. 1 (45), pp. 84-87 (in Russian).

20. Volkov D. V., Saenko I. B., Starkov A. M., Sultanbekov A. T. Ocenka ustojchivosti seti peredachi dannyh v usloviyah destruktivnyh vozdejstvij [Evaluation of the Stability of the Data Transmission Network Under Destructive Impacts]. *Izvestiya Tul'skogo Gosudarstvennogo Universiteta. Tekhnicheskie Nauki*, 2018, no. 12, pp. 358-363 (in Russian).

21. Semenov S. S., Gusev A. P., Barbot'ko N. V. Ocenka informacionno-boevogo potenciala storon v tekhnosfernyh konfliktah [Assessment of Information and Combat Potential of the Parties in Technosphere Conflicts]. *H&ES Research*, 2013, vol. 5, no. 6, pp. 10-21 (in Russian).

22. Starodubcev Yu. I., Buharin V. V., Semenov S. S. Tekhnosfernaya vojna [Technosphere War]. *Information Systems and Technologies*, 2011, no. 1, pp. 80-85 (in Russian).

23. Ivankin M. P. Tolstyh N. N., Savinkov A. Yu., Sverdel V. F. K voprosu ocenki effektivnosti funkcionirovaniya sistem programmno-opredelyaemogo radio v usloviyah informacionnogo konflikta [To the Question of Estimation of Efficiency of Functioning of Software-Defined Radio Systems in the Conditions of the Information Conflict]. *Radio Communication Theory and Equipment*, 2018, no. 4, pp. 14-18 (in Russian).

24. Hoar Ch. *Vzaimodejstvuyushchie posledovatel'nye processy* [Communicating Sequential Processes]. Moscow, Mir Publ., 1989. 264 p. (in Russian).

25. Tekunov V. V., Yazov Yu. K. Modelirovanie dinamiki realizacii ugroz bezopasnosti informacii s ispol'zovaniem apparata setej petri-markova [Modeling of Dynamics of Information Security Threats Implementation Using Petri-Markov Networks Apparatus]. *Information and Security*. 2018, vol. 21, no. 1, pp. 38-47 (in Russian).

26. Charrton-Bost B., Mattern F., Tel G. Synchronous, Asynchronous, and Casually Ordered Communication. *Distributed Comput*., 1996, vol. 9, pp. 173-191.

27. Clarke E. M., Grumberg O., Peled D. *Model Checking*. New York, MIT Press, 1999, 314 p.

28. Gan C., Yang X., Liu W., Zhu Q. A Propagation Model of Computer Virus with Nonlinear Vaccination Probability. *Communications in Nonlinear Science and Numerical Simulation*, 2014, vol. 19, no. 1, pp. 92-100.

29. Mishra B. K., Jha N. SEIQRS Model for the Transmission of Malicious Objects in Computer Network. *Applied Mathematical Modelling*, 2010, vol. 34, no. 3, pp. 710-715.

30. Hayhurst K. J., Veerhusen D. S., Chilenski J. J., Rierson L. K. A *Practical Tutorial on Modified Condition / Decision Coverage*. NASA, 2001. 85 p.

31. Peregudov M. A., Boyko A. A. Model' procedury zarezervirovannogo dostupa k srede seti paketnoj radiosvyazi [The Model of the Procedure of Reserved Access to the Packet Radio Network Environment]. *Telecommunications*, 2015, no. 6, pp. 7-15 (in Russian).

32. Peregudov M. A., Boyko A. A. Model' procedury sluchajnogo mnozhestvennogo dostupa k srede tipa S-ALOHA [The Model of the Procedure of Random Multiple Access to the Medium of S-ALOHA Type]. *Information and Control Systems*, 2014, no. 6, pp. 75-81 (in Russian).

33. Peregudov M. A., Boyko A. A. Model' procedury upravleniya pitaniem seti paketnoj radiosvyazi [The Model of the Power Management Procedure of the Packet Radio Network]. *Telecommunications*, 2015, no. 9, pp. 13-18 (in Russian).

34. Peregudov M. A., Boyko A. A. Ocenka zashchishchennosti seti paketnoj radiosvyazi ot imitacii abonentskih terminalov na urovne procedury sluchajnogo mnozhestvennogo dostupa k srede tipa S-ALOHA [Evaluation Security of Packet Radionetwork from Simulation of Subscriber Terminals at Level of Random Multiple Access Procedure to Environment of S-ALOHA Type]. *Informacionnye Tehnologii*, 2015, vol. 21, no. 7, pp. 527-534 (in Russian).

35. Peregudov M. A., Semchenko I. A. Evaluation of Efficiency of Random Multiple Access to Aloha Type Environment with Voice Connections, Transfer of Service Commands, Text Messages and Multimedia Files in Destructive Impact Conditions. *SPIIRAS Proceedings*, 2019, vol. 18, no. 4, pp. 887-911. DOI: 10.15622/sp.2019.18.4.887-911 (in Russian).

36. Peregudov M. A., Steshkovoy A. S., Boyko A. A. Veroyatnostnaya model' procedury sluchajnogo mnozhestvennogo dostupa k srede tipa CSMA/CA [The Probabilistic Random Multiple Access Procedure Model to the CSMA/CA Type Medium]. *SPIIRAS Proceedings*, 2018, no. 4, pp. 92-114. DOI: 10.15622/sp.59.4 (in Russian).

37. Zhumatij V. P., Budnikov S. A., Parshin N. V. *Ugrozy programmno-matematicheskogo vozdejstviya* [Threats of Software-mathematical Impact]. Voronezh, CPKS TZI Publ., 2010. 230 p. (in Russian).

38. Baranov S. N., Domarackij A. N., Lastochkin N. K., Morozov V. P. *Process razrabotki programmnyh izdelij* [Software Development Process]. Moscow, Nauka Publ., 2000. 176 p. (in Russian).

39. Beizer B. *Black-Box Testing*. New York, Wiley, 1995. 324 p.

40. Genel't A. E. *Upravlenie kachestvom razrabotki programmnogo obespecheniya* [Quality Management of Software Development]. Saint-Petersburg, ITMO Publ., 2007. 187 p. (in Russian).

41. Groshev S. G. Primenenie tekhnologii UniTesK dlya testirovaniya sistem s razlichnoj konfiguraciej aktivnyh potokov upravleniya [Application of UniTesK Technology for Testing Systems with Different Configurations of Active Control Flows]. *Proceedings of the Institute for System Programming of the RAS*, 2006, vol. 9, pp. 67-82 (in Russian).

42. Kaner S., Folk Dzh., Nguen E. *Testirovanie programmnogo obespecheniya* [Software Testing]. Kiev, DiaSoft Publ., 2001. 554 p. (in Russian).

43. Kulyamin V. V. *Metody verifikacii programmnogo obespecheniya* [Software Verification Methods]. Moscow, Institute for System Programming of the RAS, 2008. 111 p. (in Russian).

44. Lipaev V. V. *Testirovanie programm* [Program Testing]. Moscow, Radio i svyaz' Publ., 1986. 296 p. (in Russian).

45. Polovko A. M., Gurov S. V. *Osnovy teorii nadezhnosti* [Fundamentals of Reliability Theory]. Saint-Petersburg, BHV-Peterburg Publ., 2006. 704 p. (in Russian).

46. Tejer T. Lipov M., Nel'son E. *Nadezhnost' programmnogo obespecheniya* [Software Reliability]. Moscow, Mir Publ., 1981. 323 p. (in Russian).

47. Karpovskij E. Ya., Chizhov S. A. *Nadezhnost' programmnoj produkcii* [Reliability of Software Products]. Kiev, Tekhnika Publ., 1990. 160 p. (in Russian).

48. Myers G. J. *The Art of Software Testing*. New Jersey: John Wiley & Sons, 2004. 255 p.

49. Porteuos M., Kirakowski J., Cutts D. *Software Usability Measurement Inventory User Handbook*. Cork, Human Factors Research Group, University College, 1993. 54 p.

50. State Standard R ISO/IEC 25041-2014 *Informacionnye tekhnologii. Sistemnaya i programmnaya inzheneriya. Trebovaniya i ocenka kachestva sistem i programmnogo obespecheniya. Rukovodstvo po ocenke dlya razrabotchikov, priobretatelej i nezavisimyh ocenshchikov* [Information Technologies. Systems and Software Engineering. Systems and Software Quality Requirements and Evaluation (SQuaRE). Evaluation Guide for Developers, Acquirers and Independent Evaluators]. Moscow, Standartov Publ., 2014. 43 p. (in Russian).

51. State Standard R ISO/IEC 9126-93 *Informacionnaya tekhnologiya. Ocenka programmnoj produkcii. Harakteristiki kachestva i rukovodstva po ih primeneniyu* [Information Technology. Software Product Evaluation. Quality Characteristics and Guidelines for their Use]. Moscow, Standartov Publ., 1993. 12 p. (in Russian).

52. ISO/IEC/IEEE 29119-4: *Software and Systems Engineering. Software Testing. Part 4: Test Techniques*. ISO/IEC JTC 1/ SC 7. 139 p.

53. Vakin S. A., Shustov L. N. *Osnovy radioprotivodeistviia i radiotekhnicheskoi razvedki* [Fundamentals of Radio Countermeasures and Electronic Intelligence]. Moscow, Soviet Radio Publ., 1968. 448 p. (in Russian).

54. Vladimirov V. I., Vladimirov I. V. *Osnovy Otsenki Konfliktno-ustoichivykh Sostoianii Organizatsionno-tekhnicheskikh Sistem* (*v Informatsionnykh Konfliktakh*) [Basics of Assessing Conflict-resistant States of Organizational and Technical Systems (in Information Conflicts)]. Voronezh, Military Aviation Engineering University Publ., 2008. 231 p. (in Russian).

55. Vladimirov V. I., Likhachev V. P., Shliakhin V. M. *Antagonisticheskii konflikt radioelektronnykh sistem. Metody i matematicheskie modeli* [The Antagonistic Conflict of Electronic Systems. Methods and Mathematical Models]. Moscow, Radiotekhnika Publ., 2004. 384 p. (in Russian).

56. Vladimirov V. I., Stuchinskij V. I. Vybor sistemy pokazatelej informacionnogo prevoskhodstva v operaciyah v usloviyah dvuhstoronnej radioelektronnoj bor'by [The Choice of Indicators of Information Superiority in Operations in the Conditions of Two-Way Electronic Warfare]. *Military Thought*, 2016, no 10, pp. 33-39 (in Russian).

57. Druzhinin V. V., Kontorov D. S., Kontorov M. D. *Vvedenie v teoriiu konflikta* [Introduction to Conflict Theory]. Moscow, Radio and Communication Publ., 1989. 288 p. (in Russian).

58. Petrov A. V., Yakovlev A. A. *Analiz i sintez radiotekhnicheskih kompleksov* [Analysis and Synthesis of Radio Engineering Complexes]. Moscow, Radio and Communication Publ., 1984. 248 p. (in Russian).

59. Kozlov S. V., Karpuhin V. I., Lazarenkov S. M. *Modeli konflikta aviacionnyh sistem radioelektronnoj bor'by i protivovozdushnoj oborony* [Conflict Models of Aviation Electronic Warfare and Air Defense Systems]. Voronezh, Zhukovsky-Gagarin Air Force Academy Publ., 2013. 468 p. (in Russian).

60. Budnikov S. A., Grevcev A. I., Ivancov A. V., Kil'dyushevskij V. M., Kozirackij A. Yu., Kozirackij Yu. L., Kushchev S. S., Lysikov V. F., Parinov M. L., Prohorov D. V. *Modeli informatsionnogo konflikta sredstv poiska i obnaruzheniia* [Models of Information Conflict of Search and Detection Tools]. Moscow, Radiotekhnika Publ., 2013. 232 p. (in Russian).

61. Gubarev V. A., Krutskikh P. P. Kontseptual'naia Model' konflikta v informatsionnoi bor'be [The Conceptual Model of Conflict in the Information Struggle]. *Radiotekhnika*, 1998, no. 6, pp. 29-31 (in Russian).

62. Kuznecov V. I. *Radiosvyaz' v usloviyah radioelektronnoj bor'by* [Radio Communication in Electronic Warfare]. Voronezh, VNIIS Publ., 2002. 403 p. (in Russian).

63. Poddubnyi V. N., Agafonov A. A., Lozhkin K. Iu. Metodologiia i rezul'taty sinteza i otsenki effektivnosti prednamerennykh pomekh priemnikam diskretnykh signalov [The Methodology and Results of the Synthesis and Evaluation of the Effectiveness of Intentional Interference to Receivers of Discrete Signals]. *Journal of Communications Technology and Electronics*. 2003, vol. 48, no. 8, pp. 956-962 (in Russian).

64. Mochalov S. A. *Avtomatizirovannyj sintez mnogofunkcional'noj integrirovannoj radioelektronnoj sistemy. Metodologiya issledovaniya aviacionnyh kompleksov VMF* [Automated Synthesis of Multifunctional Integrated Electronic

System. The Research Methodology of Naval Aircraft Systems]. Moscow, Radiotekhnika Publ., 2014. 240 p. (in Russian).

65. Perunov Yu. M., Fomichev K. I., Yudin L. M. *Radioelektronnoe podavlenie informacionnyh kanalov sistem upravleniya oruzhiem* [Electronic Suppression of Information Channels of Weapon Control Systems]. Moscow, Radiotekhnika Publ., 2003. 416 p. (in Russian).

66. Agafonov A. A., Artiukh S. N., Afanas'ev V. I., Afanas'eva E. M., Bostynets I. P., Bykov V. V., Dontsov A. A., Ermakov A. I., Kalinkov A. K., Kaunov A. E., Kirsanov E. A., Laptev I. V., Lozhkin K. Iu., Marek Ia. L., Mironov V. A., Nechaev S. S., Novikov I. I., Ovcharenko L. A., Ogreb S. M., Poddubnyi V. N., Pon'kin V. A., Radzievskii V. G., Razin'kov S. N., Romanov A. D., Ryzhov A. V., Sirota A. A., Solov'ev V. V., Sorokin Iu. A., Sukhorukov Iu. S., Telkov A. Iu., Ufaev V. A., Kharchenko T. V., Iukhno P. M., Ian'shin S. N. *Sovremennaia radioelektronnaia bor'ba. Voprosy metodologii* [Modern Electronic Warfare. Methodology Issues]. Moscow, Radiotekhnika Publ., 2006. 424 p. (in Russian).

67. Cvetkov A. G. *Principy kolichestvennoj ocenki effektivnosti radioelektronnyh sredstv* [Principles of Quantitative Evaluation of Radio-electronic Means Efficiency]. Moscow, Soviet Radio Publ., 1971. 200 p. (in Russian).

68. Chikin M. G. Osobennosti ispol'zovaniya apparata polumarkovskih processov dlya modelirovaniya napravlenij radiosvyazi v interesah ocenki effektivnosti radiopodavleniya [Features of Using the Apparatus of Semi-Markov Processes for Modeling Radio Communication Directions in Order to Assess the Effectiveness of Radio Suppression]. *Radiotekhnika*, 2005, np 9, pp. 35-39 (in Russian).

69. Astapenko Yu. A., Vajpan S. N., Vakulenko A. A., Vakulenko N. N., Verba B. C., Gribkov R. A., Guzenko O. B., Dod V. N., Zajcev A. G., Zebzeev A. A., Ivanov A. N., Ionkin A. A., Korol' O. V., Kuz'min G. V., Lyaskovskij B. L., Maruhlenko A. S., Neplyuev O. N., Pristupyuk I. A., Proskurin V. I., Ryumshin A. R., Samushkin A. N., Senchakov G. V., Turko N. I., Shevchuk V. I., Shevchuk D. V., Yagol'nikov S. V. *Konfliktno-ustojchivye radioelektronnye sistemy. Metody analiza i sinteza* [Conflict-Resistant Electronic Systems. Methods of Analysis and Synthesis]. Moscow, Radiotekhnika Publ., 2015, 312 p. (in Russian).

70. Adamy D. L. EW 104: *Electronic Warfare Against a New Generation of Threats*. Boston-London, Artech House Publ., 2015. 491 p.

71. Novikov D. A. Ierarkhicheskie modeli voennykh deistvii [Hierarchical Models of Military Actions]. *Large-scale Systems Control*, 2012, no. 37, pp. 25-61 (in Russian).

72. Alekseev O. G., Anisimov V. G., Anisimov E. G. *Markovskie modeli boia* [Markov Battle Models]. Moscow, Ministry of Defense of the USSR Publ., 1985. 85 p. (in Russian).

73. Arbuzov I. V., Bolhovitinov O. V., Volochaev O. V., Vol'nov I. I., Gostev A. V., Myshkin L. V., Habirov R. N., SHekhovcov V. L. *Boevye aviacionnye kompleksy i ih effektivnost'* [Combat Aircraft Systems and their Effectiveness].

Moscow, Zhukovsky Air Force Engineering Academy Publ., 2008. 224 p. (in Russian).

74. Borisov V. V., Syskov V. V. Mul'tiagentnoe modelirovanie slozhnykh organizatsionno-tekhnicheskikh sistem v usloviiakh protivoborstva [Multi-agent Modeling of Complex Organizational and Technical Systems in the Context of Confrontation]. *Informacionnye Tehnologii*, 2012, no. 4, pp. 7-14 (in Russian).

75. Buravlev A. I., Gorshkov P. S. K voprosu o postroenii agregirovannoi modeli protivoborstva gruppirovok voisk [About the Issue of Building an Aggregated Model of Confrontation between Groups of Troops]. *Armament and Economy*, 2017, no. 5(42), pp. 35-48 (in Russian).

76. Vajner A. Ya. *Takticheskie raschety* [Tactical Calculations]. Moscow, Voenizdat Publ., 1982. 176 p. (in Russian).

77. Girin A. V. Usovershenstvovannaya metodika opredeleniya boevich vozmozhnostey obshevoiskovoy gruppirovki voisk [Improved Methodology for Determining Combat Capabilities of a Combined Arms Troop Grouping]. *Military Thought*, 2012, no. 10, pp. 26-30 (in Russian).

78. Zakharov L. V., Bogdanov S. A. O virabotke edinih podhodov k ocenke boevih potencialov [About the Development of Unified Approaches to the Assessment of Combat Potentials]. *Military Thought*, 1992, no. 8-9, pp. 42-49 (in Russian).

79. Merkulov S. N., Sukhorukov Iu. S., Donskov Iu. E. Problemy avtomatizatsii intellektual'noi podderzhki priniatiia reshenii obshchevoiskovymi komandirami v takticheskom zvene [Problems of Automation of Intellectual Decision Support by Combined-arms Commanders at the Tactical Level]. *Military Thought*, 2009, no. 9, pp. 43-53 (in Russian).

80. Mitiukov N. V. *Imitatsionnoe modelirovanie v voennoi istorii* [Simulation in Military History]. Moscow, LENAND Publ., 2018. 280 p. (in Russian).

81. Polenin V. I., Sushchenkov D. A. Razrabotka modeli vooruzhennogo protivoborstva boevykh sistem takticheskogo urovnia s naneseniem udarov neposredstvenno po boevoi sisteme protivnika i otrazheniem udarov protivnika po svoei boevoi sisteme [Development of a Model of Armed Confrontation of Combat Systems at the Tactical Level with Striking Directly at the Enemy's Combat System and Repelling the Enemy's Strikes Against its Combat System]. *National Association of Scientists*, 2015, no. 8 (17), pp. 167-171 (in Russian).

82. Sosura O. V. *Raschet obobshennich pokazateley boevich vozmozhnostey voisk v operachiyach (boevich deistviyah) s uchetom effectivnosti upravleniya imi (potencialno-delevoy metod)* [Calculation of Generalized Indicators of the Combat Capabilities of Troops in Operations (Combat Operations), Taking into Account the Effectiveness of their Management (the Potential-share Method)]. Moscow, Military Thought Publ., 1997. 142 p. (in Russian).

83. Tarakanov K. V. *Matematika i vooruzhennaya borba* [Mathematics and Armed Struggle]. Moscow, Voenizdat Publ., 1974. 240 p. (in Russian).

84. Tkachenko P. N., Kutsev L. N., Meshcheriakov G. A., Chavkin A. M., Chebykin A. D. *Matematicheskie modeli boevykh deistvii* [Mathematical Models of Fighting]. Moscow, Soviet Radio Publ., 1969. 240 p. (in Russian).

85. Fendrikov N. M., Iakovlev V. I. *Metody raschetov boevoi effektivnosti vooruzheniia* [Calculation Methods of Combat Effectiveness of Weapons]. Moscow, Voenizdat Publ., 1971. 224 p. (in Russian).

86. Chernoskutov A. I., Sitkevich A. V., Trishkin V. S. Ratsional'nyi sposob unichtozheniia raznorodnykh gruppirovok [Rational Way to Destroy Dissimilar Groups]. *Military Thought*, 2018, no. 1, pp. 63-67 (in Russian).

87. Chuev Iu. V. *Issledovanie operatsii v voennom dele* [Operations Research in Military]. Moscow, Voenizdat Publ., 1970. 256 p. (in Russian).

88. Chowdhury S. M., Kovenock D., Sheremeta R. M. An Experimental Investigation of Colonel Blotto Games. *CESifo Working Paper*, 2009, no. 2688, 36 p.

89. Washburn A., Kress M. *Combat Modeling*. London, Springer Publ., 2009. 281 p.

90. Kress, M. Caulkins J. P., Feichtinger G., Grass D., Seidl A. Lanchester Model for Three-way Combat. *European Journal of Operational Research*, 2018, no. 1 (264), pp. 46-54.

91. Kalinin V. N., Reznikov B. A., Varakin E. I. *Teoriia sistem i optimal'nogo upravleniia. Chast' 2. Poniatiia, modeli, metody i algoritmy optimal'nogo vybora* [System Theory and Optimal Control. Part 2. Concepts, Models, Methods and Algorithms for Optimal Choice]. Moscow, Ministry of Defense of the USSR Publ., 1987. 589 p. (in Russian).

92. Makarenko S. I. *Spravochnik nauchnyh terminov i oboznachenij* [The Reference Book of Scientific Terms and Symbols]. Saint Petersburg, Naukoemkie tekhnologii Publ., 2019. 254 p. (in Russian).

93. Boyko A. A., Obushchenko E. Yu., Scheglov A. V. Osobennosti sinteza polnogo mnozhestva testovyh sposobov udalennogo informacionno-tekhnicheskogo vozdejstviya na prostranstvenno raspredelennye sistemy informacionno-tekhnicheskih sredstv [Features of Synthesis of a Full Set of Test Methods of Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Means]. *Bulletin of Voronezh State University. Series: Systems Analysis and Information Technology*, 2017, no. 2, pp. 33-45 (in Russian).

94. Boyko A. A., Hramov V. Yu. Metodika ocenki pravil'nosti i ustojchivosti k oshibkam special'nogo programmnogo obespecheniya avtomatizirovannyh sistem voennogo naznacheniya [The Methods of Evaluation of Correctness and Error Tolerance of Special Software of Military Automated Systems]. *Bulletin of Voronezh State University. Series: Systems Analysis and Information Technology*, 2007, no 1, pp. 106-115 (in Russian).

95. Boyko A. A., Hramov V. Yu. Metodika ocenki prigodnosti special'nogo programmnogo obespecheniya avtomatizirovannyh sistem i sredstv upravleniya REB [The Methods of Evaluation of Suitability of Special Software for EW Automated Systems and Means]. *Bulletin of Military Institute of Radioelectronics*, 2007, no. 1 (6), pp. 218-225 (in Russian).

96. Boyko A. A., Hramov V. Yu. Formirovanie testovyh posledovatel'nostej vypolneniya informacionno-raschetnyh zadach pri ocenke chastnyh pokazatelej kachestva special'nogo programmnogo obespecheniya [Formation of Test Sequences of Information and Calculation Tasks in the Evaluation of Private Indicators of the

Quality of Special Software]. *Sbornik trudov Vserossijskoj nauchno-tekhnicheskoj konferencii ad"yunktov, aspirantov, soiskatelej i molodyh specialistov* [Proceedings of the All-Russian Scientific and Technical Conference of Adjuncts, Graduate Students, Applicants and Young Professionals]. Voronezh, FGNIIC REB OESZ Publ., 2008, pp. 295-301 (in Russian).

97. Boyko A. A., Djakova A. V. The Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools. *Information and Control Systems*, 2014, no. 3, pp. 84-92 (in Russian).

98. Boyko A. A. The Evaluation Method of Armament Samples Informatization Level. *Systems of Control, Communication and Security*, 2019, no. 1, pp. 264-275. DOI: 10.24411/2410-9916-2019-10116 (in Russian).

99. Boyko A. A. Sposob stratificirovannogo analiticheskogo opisaniya processa funkcionirovaniya informacionno-technicheskih sredstv [The Stratified Analytical Description Method of the Functioning Process of Information-Technical Tools]. *Informacionnye Tehnologii*, 2015, no. 1, pp. 35-42 (in Russian).

100. Boyko A. A., Budnikov S. A. The Model of Information Conflict between Special Software and Information Security Subsystem of Information-Technical Tool. *Radiotekhnika*, 2015, no. 4, pp. 136-141 (in Russian).

101. Klejnrok L. *Vychislitel'nye sistemy s ocheredyami* [Computing Systems with Queues]. Moscow, Mir Publ., 1979. 600 p. (in Russian).

102. Boyko A. A. The Analytical Modeling Method of the Virus Propagation Process in Computer Various Structures Networks. *SPIIRAS Proceedings*, 2015, no. 5, pp. 196-211 (in Russian).

103. Boyko A. A., Degtyarev I. S. The Weight Coefficient Estimation Method of Elements in Organizational and Technical Systems. *Systems of Control, Communication and Security*, 2018, no. 2, pp. 245-266 (in Russian).

104. Boyko A. A. The Warfare Analytical Modeling Method. *Systems of Control, Communication and Security*, 2019, no. 2, pp. 1-27. DOI: 10.24411/2410-9916-2019-10201 (in Russian).

105. Boyko A. A. O zashishennosti informacii voinskih formirovaniy v sovremennom vooruzhennom protivoborstve [About the Information Security of Military Formations in the Modern Armed Confrontation]. *Military Thought*, 2016, no. 4, pp. 38-51 (in Russian).

106. Boyko A. A., Hramov V. Yu. The Model of Information Conflict between Information-Technical Means and Special Software in Armed Confrontation of Groups with Static Characteristics. *Radiotekhnika*, 2013, no. 7, pp. 5-10 (in Russian).

107. Boyko A. A. The Method of Developing Hierarchic Multy-level Models for Analytical Assessment of the Correlation of Forces in Military Formations // *Military Thought*, 2019, no. 7, pp. 104-113 (in Russian).

Статья поступила 30 сентября 2019 г.

Информация об авторах

Бойко Алексей Александрович – кандидат технических наук, доцент. Докторант. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сложных систем. E–mail: albo@list.ru

Будников Сергей Алексеевич – доктор технических наук, доцент. Начальник кафедры автоматизированных систем управления и информационной безопасности. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сложных систем. E–mail: buser@bk.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

Conflict Resistance Ensuring of Software Implementation of Control Algorithms of Radioelectronic Equipment of Spatially Distributed Organization and Technical Systems

A. A. Boyko, S. A. Budnikov

Problem Statement. *The processes of functioning of radioelectronic equipment in the antagonistic conflict of spatially distributed heterogeneous organizational and technical systems are characterized by diversity, variability and low predictability. The quality of software implementation of control algorithms for radioelectronic equipment has a significant influence on the capabilities of such systems. However, the known methods of synthesis of organizational and technical systems do not take into account this influence.* ***Aim of the paper*** *is to ensure the conflict resistance of software implementation of control algorithms of radioelectronic equipment of spatially distributed organization and technical systems. The identification of the external and internal specific for telecommunication protocols and program man-machine interfaces program security threats of the set sample of radioelectronic equipment and the definition of these threats, which elimination will provide increase or achievement of required level of the target efficiency of equipment's organizational and technical system in the conflict are the parts of the obtained method, which* ***is the idea of the work. Novelty:*** *the possibility of evaluation of the quality of software implementation of control algorithms of radioelectronic equipment on the course and outcome of the antagonistic conflict of organizational and technical systems where this equipment is used is obtained.* ***Result:*** *the proposed method transforms into techniques of substantiation of numerical values of parameters of functional suitability, performance efficiency, reliability and security of software implementation of control algorithms of radioelectronic equipment of spatially distributed heterogeneous organizational and technical systems. The example of application of a technique of substantiation of requirements to functional suitability of software implementation of control algorithms of radioelectronic equipment for two equal battalions battle with various informatization level* Δ *is shown. It is discovered that functional suitability of the software implementation of control algorithms for radioelectronic equipment of the battalion in the defense must be not less than 0.32 when* $\Delta=0.5$*, not less than 0,53 when* $\Delta=0.6$*, not less than 0,65 when* $\Delta=0,7$*, not less than 0,72 when* $\Delta=0.8$*, not less than 0,77 when* $\Delta=0.9$ *and not less than 0,81 when* $\Delta=1$*.* ***Practical relevance.*** *The solution can be used when the modernization of existing means and the creation of perspective samples of conflict-resistant radioelectronic equipment are needed.*

Keywords*: radioelectronic equipment, antagonistic conflict, resistance, organization and technical system, software threat, control algorithm.*

Information about Authors

Aleksey Aleksandrovich Boyko – Ph.D. of Engineering Sciences, Associate Professor. Doctoral Candidate. Zhukovsky and Gagarin Military Aviation Academy. Field of research: methods and systems of information protection, methods of assessing the effectiveness of complex systems. E–mail: albo@list.ru

Sergey Alekseevich Budnikov – Advanced Doctor, Docent. Head of the Department of Automated Control Systems. Zhukovsky and Gagarin Military Aviation Academy. Field of research: information security, modeling of complex systems. E–mail: buser@bk.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.