

# МОДЕЛЬ СЛОЖНОГО ИНФОРМАЦИОННОГО КОНФЛИКТА ДЛЯ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Головской В. А.<sup>1</sup>

DOI: 10.21681/2311-3456-2025-1-86-95

**Цель работы:** формализация модели сложного информационного конфликта и конструктивное доказательство повышения информативности модели такого конфликта, усовершенствованной путем включения в нее индифферентного информационного взаимодействия.

**Методы исследования:** общенаучные методы – абстрагирование, обобщение, анализ и методы теории алгоритмов и теории информации.

**Результат исследования:** формализована известная модель сложного информационного конфликта информационно-технических систем, осуществлено её качественное усовершенствование для условий функционирования робототехнических комплексов. Предложено измерять информативность формализованных моделей непосредственно, а не косвенно – через моделирование влияния используемых моделей на качество функционирования системы. С привлечением абстракций отождествления и потенциальной осуществимости, традиционных для теоретико-алгоритмических построений, обоснован подход к использованию колмогоровской сложности для количественного оценивания качественного усовершенствования рассматриваемой модели сложного информационного конфликта. Получены аналитические выражения, позволяющие, оценивать информативность предложенных моделей.

**Практическая ценность:** представленные результаты обеспечивают возможность решения задач оценивания достаточности средств защиты информации и выбора конфликтно-устойчивого состояния радиосистемы, а также расширяют спектр методов, используемых при исследованиях информационных конфликтов.

**Ключевые слова:** антагонистический конфликт, информационное взаимодействие, количество информации, радиоэлектронный конфликт, колмогоровская сложность.

## Введение

В работе исследуется информационный конфликт как условие функционирования радиосистемы робототехнического комплекса, рассматриваемого экспертами<sup>2</sup> как средство повышения эффективности вооруженного противоборства, становящегося все более сложным и динамичным [1, 2].

Под РТК далее понимается информационно-техническая система (ИТС), включающая в себя [3] группу робототехнических средств (РТС), радиосистему передачи данных (РС), сопряженную с подсистемой защиты информации (ЗИ) РТК, а также пункт управления.

РТС обладают рядом ограничений [3, 4], наследуемых их подсистемами. Такими ограничениями являются массогабаритные характеристики и емкость источников питания, что накладывает, в свою очередь, ограничения на время автономной работы, вычислительные возможности подсистем и т.д. Одной из подсистем РТК, наиболее зависимой от ограничений и в то же время функционирующей в условиях конфликта со средой, является его РС. Полагаем, что РС РТК обеспечивает [3] передачу по радиоканалам разнородных данных как между РТС и пунктом управления, так и между РТК и коалиционными системами,

т.е. объединенными в условную «коалицию» согласованностью своих целей функционирования с целями надсистемы [3].

Развитие теории и практики информационного противоборства [1, 5, 6] обуславливает как ужесточение требований к конфликтной устойчивости РС РТК [3, 6] и защищенности циркулирующей в радиоканалах этих РС информации, так и актуальность исследований по обеспечению указанных требований в условиях информационного конфликта (ИК).

Для обеспечения защищенности передаваемой по радиоканалам РС информации могут применяться криптографические или некриптографические средства, обладающие специфическими особенностями [7]. В работе [8] сформулирована актуальная проблема оценивания достаточности средств ЗИ и показана необходимость использования формальной модели ИК для разрешения соответствующей алгоритмической проблемы. Однако подходящая для этой цели модель ИК в настоящее время отсутствует [8].

Одним из способов обеспечения конфликтной устойчивости РС в условиях реализуемой антагонистической стороной ИК активной электромагнитной

1 Головской Василий Андреевич, кандидат технических наук, доцент, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: golovskoy\_va@mail.ru

2 Science & Technology Trends 2023-2043. NATO Science & Technology Organization. Volume 1: Overview. <https://cesmar.it/wp-content/uploads/2023/04/stt23-vol1.pdf>

деятельности при наличии ряда критичных ограничений, характерных для РТК, является повышение информированности подсистемы управления ресурсами [9] об условиях среды функционирования. Исследователями рассматриваются два основных направления повышения информированности: экстенсивное, характеризующееся всеобъемлющей интеграцией коалиционных ИТС [5], и интенсивное, заключающееся в повышении информативности моделей и эффективности их использующих алгоритмов управления ресурсами [4, 5, 9], например, когнитивного управления [5]. В русле второго направления совершенствование моделей осуществляется за счет введения в них новых сущностей или связей [3, 10]. Такое совершенствование призвано обеспечить более полное описание явлений объективной реальности, что объясняет увеличение количества информации, содержащейся в модели. При предложенной выше дихотомии сделано естественное предположение, что увеличение количества информации, поступающей на вход ИТС, улучшает качество функционирования указанной системы, понимаемое в широком смысле и далее в работе подлежащее пояснению. Однако в доступных автору источниках отсутствуют подходы к количественному оцениванию информативности моделей ИК.

Предлагаемая статья, являясь развитием работ [3, 11], посвящена построению формальной модели ИК, которая при наполнении ее конкретными данными будет являться непосредственно входом для соответствующих алгоритмов, и оцениванию информативности различных описаний ИК.

### 1. Постановка задачи

Рассмотрим в качестве условий функционирования РС РТК содержание информационного и радиоэлектронного конфликтов. Известна [10, 12] вложенность последнего в ИК, под которым понимается [13] «процесс столкновения ИТС на этапе сбора и обработки данных о состоянии, намерениях и действиях противостоящей стороны, каждая из которых стремится упреждающему принятию управленческих решений по отношению к противостоящей стороне и предпринимает определенные действия по снижению возможностей противостоящих средств сбора и обработки данных». Вследствие указанной вложенности понятий «информационное взаимодействие» (ИВ) является более широким [3, 14], чем используемый термин «радиоэлектронное взаимодействие». Далее для построения формальной модели ИК при описании взаимодействий ИТС будет использоваться термин ИВ, учитывающий вложенность в него «радиоэлектронного взаимодействия».

По типам возникающих между сторонами конфликта ИВ выделяют [15] коалиционный и антаго-

нистический ИК. Антагонистический ИК определяют [6, 11] как «процесс ИВ сторон ИК, имеющих противоположные цели и стремящихся достигнуть несовместимых состояний». Указанные цели ИТС раскрываются при информационном анализе радиоэлектронной борьбы [16], осуществляемой с целью «обеспечения доступа к электромагнитному спектру своим пользователям и осложнения/запрещения доступа пользователям противоположной стороны ИК» [16]. Коалиционный ИК объясняется нарушением электромагнитной совместимости<sup>3</sup> РС с системами, отнесенными к коалиции.

Исследования ИК ИТС – предмет множества работ, в которых ИК рассматривается, как правило, с позиций антагонистического ИК [1, 2], либо с позиций коалиционного [18], и как исключение рассматриваются оба типа ИВ [15]. Анализ подходов к исследованию ИК посвящен подробный обзор<sup>4</sup>, а формализации их моделей – работы [17, 19], в которых, как и в подавляющем большинстве рассмотренных работ, акцент делается на антагонистическом ИК.

В монографии<sup>5</sup> предложена описательная модель сложного ИК (СИК), отличающаяся одновременным учетом антагонистического и коалиционного типов конфликтных ИВ ИТС с объектом взаимодействия, однако данная модель не была формализована. В работе [3] предложено расширение указанной модели СИК, заключающееся во введении в рассмотрение еще одного типа ИВ, в дополнение к антагонистическому и коалиционному, существенного для исследуемой проблемы обеспечения конфликтной устойчивости РС РТК, – индифферентного ИВ. Указанное расширение при этом обосновывалось индуктивно, и конструктивного доказательства его достоинств дано не было. В монографии [17] индифферентный тип ИВ выведен из рассмотрения ввиду декларируемой практической возможности его устранения. В докладе [11] показана согласованность расширения [3] известной модели СИК с графовой моделью [9] когнитивной РС (КРС) и с методологией обучения с подкреплением, рассматриваемой в качестве приоритетной при создании КРС [9], а также представлены предложения по использованию алгоритмического подхода к количественному оцениванию эффективности указанного качественного

3 Козирацкий Ю. Л., Иванцов А. В., Мамаджанян Е. А. Метод оперативной оценки радиоэлектронной обстановки в интересах обеспечения скрытности и электромагнитной совместимости радиоэлектронных средств // Журнал Сибирского федерального университета. Серия: Техника и технологии. 2018. № 3. С. 256–262.

4 Макаренко С. И., Михайлов Р. Л. Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95–178.

5 Астапенко Ю. А. и др. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза / Под ред. С. В. Ягольникова. – М.: Радиотехника, 2015. 312 с.

усовершенствования модели СИК. Однако в [11] не представлен способ описания ИК, а формализация ограничена только описанием рассматриваемых типов ИВ.

Необходимо отметить, что формализация необходима не только для устранения известной семантической неполноты вербальных моделей. Формализованная модель, при наполнении её конкретными данными, способна служить источником информации непосредственно для подсистем управления [9], а также – для разработчиков как конфликтно-устойчивых ИТС в целом [15], так и их подсистем ЗИ [8]. Так, например, система обучения с подкреплением способна сформировать модель среды, однако неверные послышки, получаемые от подсистемы логического вывода, могут привести к неточной модели или к более трудному нахождению оптимального решения. В работе [9] была предложена модель подсистемы управления КРС, использующая логический вывод для получения знаний о среде, необходимых для обеспечения конфликтной устойчивости КРС. Также предлагалось [9] формировать знания на основе информации, заложенной в подсистему и поступающей при функционировании управляемой системы, при этом были показаны [9] подходы к использованию информации о ИК для формирования решения о выборе конфликтно-устойчивого состояния. Однако в работах [3, 9] было приведено достаточно общее содержание требуемых данных о среде и ИК, что было частично устранено при попытке построения формальной модели ИК [11] и использовании ее в качестве входа для алгоритма прогнозирования.

С учетом приведенных аргументов повышение качества, указанное в сформулированном выше предположении, может быть интерпретировано как повышение эффективности расходования ресурсов при вычислении решения задачи, или же – повышение точности этого решения. Примером описываемого явления может служить различающаяся эффективность алгоритма на разных входах, что наблюдается у алгоритмов поиска элемента массива на несортированных и сортированных входных данных.

## 2. Основная часть

Несмотря на декларируемую экспертами [6] невозможность построения законченной теории ИК, практика, обусловленная развитием средств информационного противоборства, требует как уточнения моделей, так и расширения условий их применимости. Следует отметить, что указанное требование совершенствования моделей характерно для всех сфер деятельности, использующих моделирование [20]. При совершенствовании модели необходимо соблюдение баланса между требуемыми от нее низкой сложностью и высокой адекватностью [11]. Тогда

цель совершенствования модели может быть сформулирована как увеличение количества информации, получаемой субъектом моделирования в результате применения модели [11], либо как нахождение более короткой записи модели при той же её информативности для пользователя<sup>6</sup>. Необходимым является определение условий и правил использования модели, от которых будет зависеть выделение из среды объекта исследования, которым в настоящей работе является функционирование РС РТК в условиях ИК. Предмет исследования – информационные взаимодействия, возникающие при ИК с участием РС РТК.

Рассмотрим содержание ИК и место в нем РС РТК. Разделяемым ресурсом является радиочастотный спектр в рассматриваемой области пространства, с использованием которого осуществляется ИВ между сторонами ИК [3, 5]. Информация о состоянии спектра необходима для формирования модели среды и прогнозирования ИК, обеспечивающих решение задачи выбора конфликтно-устойчивого состояния КРС [9], а также – для выбора средств ЗИ в радиоканалах [8]. С учетом этих аргументов модель ИК с участием РС РТК формализована с использованием методологической схемы, описываемой кортежем<sup>7</sup>

$$M = \langle ES, SM, T, IM, L \rangle, \quad (1)$$

где:  $ES$  – радиочастотный диапазон электромагнитного спектра в области функционирования РС, представляющий собой объект-оригинал;  $SM$  – субъект моделирования, которым в зависимости от дальнейшего предназначения модели может быть подсистема управления ресурсами РС РТК или же система поддержки принятия решений конструктора системы ЗИ;  $T$  – цель моделирования, которая с учетом изложенного выше может быть сформулирована как обеспечение информацией субъекта моделирования;  $IM$  – инфраструктура моделирования, предоставляемая мастер-системой, выделенной на структурном уровне [9] из КРС РТК или указанной выше системой поддержки принятия решений;  $L$  – язык описания отношения объект-модель, обеспечивающий отображение  $ES$  в его конечное описание

$$L: ES \rightarrow code(ES),$$

который и является определяющим информативностью модели ИК элементом.

Очевидным примером  $L$  для получения описания  $code(ES)$  являются алгоритмы, реализуемые в современных средствах спектрального анализа. Описание  $ES$  на их выходе будет конечным, однако

6 Верещагин Н. К., Успенский В. А., Шень А. Колмогоровская сложность и алгоритмическая случайность. – М.: МЦНМО, 2013. 576 с.

7 Волкова В. Н., Козлов В. Н., Магер В. Е., Черненькая Л. В. Классификация методов и моделей в системном анализе // Сборник докладов XX Международной конференции по мягким вычислениям и измерениям. – СПб.: СПбГЭТУ(ЛЭТИ), 2017. – С. 223–226.

не обеспечит достижение цели  $T$ , т.к. отражает текущее состояние  $ES$ , однако не обладает достаточной для прогнозирования ИК информативностью о природе конфликтных ИВ [20].

При моделировании ИК и оценивании характеристик его сторон используются различные подходы [9], отличающиеся, в том числе, требуемыми наборами исходных данных о его сторонах и, соответственно, принятыми уровнями абстракции. Однако участие в ИК перспективных ИТС, в том числе интеллектуальных [1], ограничивает возможность применения многих из указанных подходов ввиду отсутствия достаточно полных описаний предполагаемых конструктивных решений и методов управления ресурсами. В этой ситуации представляется адекватным применение теоретико-алгоритмического подхода, зарекомендовавшего себя эффективным при исследованиях гипотетических систем [9, 21], представленных описаниями нетривиальных семантических свойств их реализующих алгоритмов. С учетом привлеченных абстракций и известной алгоритмической природы составляющих антагонистического ИК [1, 12] представляется целесообразным использовать традиционные для теории алгоритмов обозначения:  $code(X) \in \Sigma^*$  – слово определенной структуры конечной длины в алфавите  $\Sigma$ , кодирующее объект  $X$ ;  $A_D^C(x, y) = z$  – алгоритм, выполняющий задачу  $D$  в интересах стороны ИК  $C$ , останавливается на входе с результатом  $z$ .

Опишем условия, отличающие СИК от традиционно рассматриваемых дуэльных ситуаций и проблемы электромагнитной совместимости. При моделировании СИК предложено [15] рассматривать одновременно два типа конфликтных ИВ: антагонистическое и коалиционное (рис. 1). Известно [12], что реализация активного антагонистического ИВ одной стороной ИК в отношении элемента другой может быть осуществлена только на основании результатов успешно проведенных радиомониторинга и идентификации последнего, что согласуется и с известными моделями кибератак [22]. Будем далее в качестве допущения рассматривать только такой подход к организации ИВ антагонистической стороной ИК.

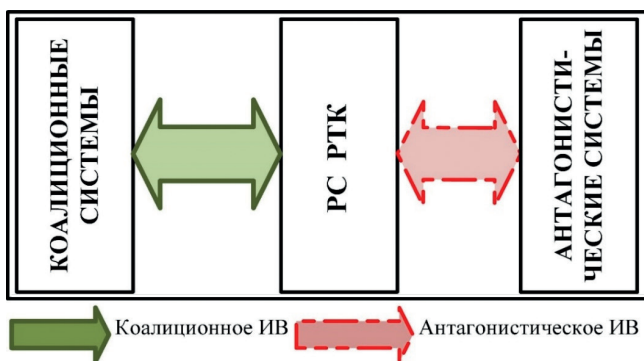


Рис. 1. Информационные взаимодействия при ИК

С учетом современных взглядов на информационное противоборство [5, 12, 16], принятых абстракций и допущений реализация антагонистического ИВ может быть представлена последовательностью событий, которым поставлены в соответствие следующие высказывания:

$$S_{RM}^A \Leftrightarrow \exists A_{RM}^A : A_{RM}^A (code(ES)) = D_{RM}; \quad (2)$$

где  $S_{RM}^A$  – обнаружение антагонистической стороной ИК факта функционирования РС РТК, описываемого набором данных  $D_{RM}$  о РС, в результате радиомониторинга, реализуемого соответствующим алгоритмом  $A_{RM}^A$

$$S_{Id}^A \Leftrightarrow \exists A_{Id}^A : A_{Id}^A (D_{Apr}^A, D_{RM}) = D_{Id}; \quad (3)$$

где  $S_{Id}^A$  – успешная идентификация антагонистической стороной ИК режима работы РС, реализуемая алгоритмом  $A_{Id}^A$ ;  $D_{Apr}^A$  – априорные данные, позволяющие антагонистической стороне вычислить идентификационные данные  $D_{Id}$  РС;

$$S_D^A \Leftrightarrow \exists A_D^A : A_D^A (D_{Apr}^A, D_{Id}) = ES_d^A; \quad (4)$$

где  $S_D^A$  – реализация целевого активного ИВ алгоритмом  $A_D^A$  в отношении выявленных в результате идентификации ресурсов РС;  $ES_d^A$  – состояние  $ES$ , при котором к нему осложнен/запрещен доступ пользователям противоположной стороны ИК. Далее для состояний  $ES$  будут использоваться записи  $ES_d^A$  или  $ES_d^C$  обозначающие, что  $ES$  перешел в них результате антагонистического ИВ или коалиционного ИВ соответственно.

Для формализации антагонистического ИВ с учетом теории и практики информационного противоборства [5, 12, 16] сформируем высказывание

$$K_A \Leftrightarrow S_D^A \vee S_{Id}^A; \quad (5)$$

т.е. считаем, что антагонистическое ИВ имеет место ( $K_A$ ), только если антагонистическая сторона осуществила радиомониторинг и/или радиоподавление КРС. Тогда последовательность событий (2)–(4) может быть адекватно описана композицией формирующих эти события алгоритмов

$$A_D^A (A_{Id}^A (A_{RM}^A (code(ES)))) = ES_d^A$$

При построении условия (5) умышленно не было учтено ИВ, обусловленное влиянием работы телекоммуникационных систем антагонистической стороны ИК, что будет сделано и пояснено ниже.

Коалиционные ИВ с учетом трех основных типов задач, решаемых коалицией, могут быть описаны при помощи трех высказываний. Влияние коалиционных ИВ на  $ES$  ввиду функционирования телекоммуникационных систем, управляемых алгоритмом  $A_{TM}^C$ , формализуемо следующим высказыванием:

$$S_{TM}^C \Leftrightarrow \exists A_{TM}^C : A_{TM}^C (D_{Apr}^C, code(ES)) = ES_d^C. \quad (6)$$



Получение данных о состоянии  $ES$  и о носителях средств радиомониторинга ( $D_I$ ) алгоритмом  $A_I^C(D_{App}^C, code(ES))$ , а также реализация алгоритмом  $A_D^C$  активного ИВ описываются соответствующими высказываниями

$$S_I^C \Leftrightarrow \exists A_I^C : A_I^C(D_{App}^C, code(ES)) = D_I D_{RM},$$

$$S_D^C \Leftrightarrow \exists A_D^C : A_D^C(D_{App}^C, code(ES)) = ES_d^C.$$

Высказывание о существовании коалиционного ИВ ( $K_C$ ) может быть формализовано следующим условием, поскольку для рассматриваемого ИК играют роль только события, соответствующие высказываниям  $S_{TM}^C$  и  $S_D^C$ :

$$K_C \Leftrightarrow S_{TM}^C \vee S_D^C. \quad (7)$$

Далее предполагается, что  $S_d^C \neq S_d^A$  и  $code(ES_d^C) \neq code(ES_d^A)$ , однако  $A_D^C(D_{App}^C, code(ES_d^A)) = ES_d^{C,A}$ ,  $A_D^A(D_{App}^A, code(ES_d^C)) = ES_d^{A,C}$  и  $ES_d^{A,C} \approx ES_d^{C,A}$ , но  $code(ES_d^{A,C}) = code(ES_d^{C,A})$ . С учетом этого предположения и принятых абстракций сформулируем критерий отнесения ИК к сложному согласно [15]

$$\Omega_K \Leftrightarrow K_C \wedge K_A. \quad (8)$$

Рассмотрим содержание усовершенствования модели СИК, реализованного путем введения в рассмотрение индифферентного ИВ [3]. Данный тип ИВ обуславливает ИК, заключающийся в нарушении электромагнитной совместимости РС РТК с техническими системами, не относящимися ни к коалиционным, ни к антагонистическим [3]. Предложено [3] называть такой конфликт индифферентным, а технические системы, участвующие в индифферентном ИК с системами РС РТК, – индифферентными. Такими индифферентными системами могут быть работающие в активном режиме [3, 11] радиорелейные и радиолокационные станции, средства подвижной радиосвязи, земных станций спутниковой связи, радиовещательных станций, а также телекоммуникационные системы антагонистической стороны ИК, если они не осуществляют целевого воздействия на РС РТК.

С учетом рассмотренных условий функционирования РТК предложено [3] выделить следующие объекты ИВ с РС РТК (рис. 2):

- антагонистические системы (информационного противоборства);
- коалиционные системы;
- индифферентные системы и часть среды функционирования РТК, оказывающая влияние на распространение радиоволн.

Выделение лишь части среды в качестве объекта ИВ объясняется влиянием условий распространения радиоволн на характеристики ИК [9] и соответствует известным положениям онтологии проектирования<sup>8</sup>.

<sup>8</sup> Боргест Н. М. Научный базис онтологии проектирования // Онтология проектирования. 2013. № 1(7). С. 7–25.

При этом актуализируется [11] вопрос о целесообразности введения новой сущности в модель (8), т.е. о нахождении баланса между её сложностью и адекватностью с учетом того, что индифферентное ИВ вносит наименьший вклад в формируемый ИК по сравнению с другими ИВ. Отметим, что необходимость выделения индифферентного ИВ обусловлена тем, что оно может быть самостоятельно описано после соответствующего наблюдения и выявления регламента работы индифферентных систем или получения их технического описания, в то время как антагонистическое ИВ является достаточно непредсказуемым и может изменяться как по причине следования тактике и её развития, так и по причине наращивания интеллектуальных способностей систем информационного противоборства [1, 5].

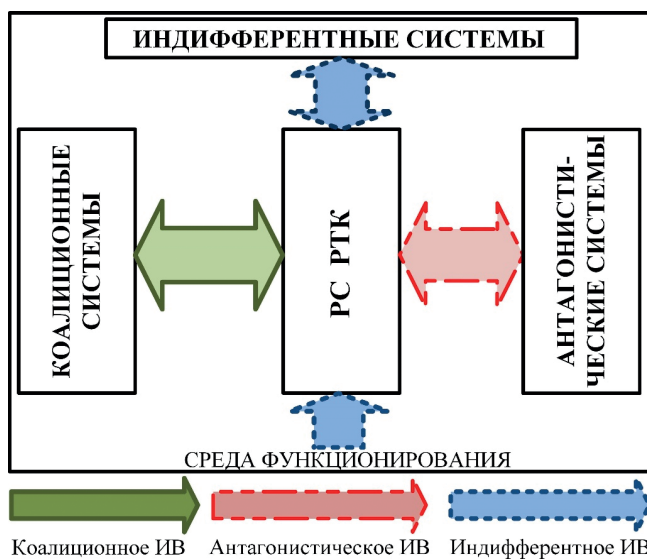


Рис. 2. Информационные взаимодействия при сложном ИК

С учетом приведенного обоснования природы индифферентного ИВ его влияние может быть описано по аналогии с (2)-(4) при помощи высказывания

$$S_{TM}^I \Leftrightarrow \exists A_{TM}^I : A_{TM}^I(code(ES)) = ES_d^I$$

Высказывание о существовании индифферентного ИК ( $K_I$ ) формализуем условием

$$K_I \Leftrightarrow S_{TM}^I. \quad (9)$$

С учетом введенного индифферентного ИВ по аналогии с (8) сформулируем высказывание об условиях отнесения ИК к сложному

$$\Omega_{K+} \Leftrightarrow K_C \wedge K_A \wedge K_I. \quad (10)$$

приняв допущения, что  $ES_d^I \neq ES_d^C \neq ES_d^A$  и  $code(ES_d^I) \neq code(ES_d^C) \neq code(ES_d^A)$ , однако  $A_{TM}^I(D_{App}^C, code(ES_d^{C,A})) = ES_d^{I,C,A}$ ,  $A_{TM}^I(D_{App}^A, code(ES_d^{A,C})) = ES_d^{I,A,C}$  и  $ES_d^{I,A,C} \approx ES_d^{I,C,A} \approx \dots \approx ES_d^{C,A,I}$ , но  $code(ES_d^{I,A,C}) = code(ES_d^{I,C,A}) = code(ES_d^{C,A,I})$ .

Иллюстрация формирования ИК с учетом принятых допущений осуществлена с использованием аппарата теории графов (рис. 3), выбранного по причине обеспечения наглядности, а также адекватности для моделирования ИК [10] и изучения причинно-следственных связей [23], необходимых для описания процесса.

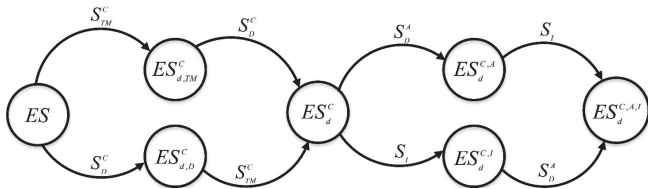


Рис. 3. Модель возникновения ИК

Разделяемый ресурс ( $ES$ ) в результате воздействия одной из составляющих коалиционного ИК (7) может перейти из бесконфликтного состояния  $ES$  в одно из состояний  $ES_{a, TM}^c$  или  $ES_{a, D}^c$ , обусловленных соответствующими ИВ  $S_{TM}^c$  или  $S_D^c$ , что иллюстрируют помеченные дуги. Дальнейший переход в новое состояние  $ES_a^c$ , описываемое условием (7), из состояний  $ES_{a, TM}^c$  или  $ES_{a, D}^c$  может быть инициирован рассмотренными уже ИВ  $S_D^c$  или  $ES_{TM}^c$ , соответственно. Формирование СИК согласно модели (8) отражает переход между состояниями  $ES_a^c$  и  $ES_{a, A}^c$  по причине антагонистического ИВ  $S_D^A$ , а индифферентное ИВ  $S_I$  обуславливает формирование СИК согласно (10) из  $ES_{a, A}^c$ . Также состояние  $ES_{a, A, I}^c$  может быть получено из  $ES_a^c$  по причинам ИВ  $S_D^A$  и  $S_I$ , обусловившего состояние  $ES_{a, I}^c$ .

Далее необходимо построить конструктивные объекты из рассмотренных выше описательных моделей ИК, которые могут быть непосредственно использованы  $IM$  в вычислениях для достижения  $T$ .

Известную описательную модель СИК (рис. 1), сущность которой отражает сформированное условие (8), предлагается формализовать с помощью отображения

$$L_K : ES \rightarrow code(ES_{a, C}^A), \quad (11)$$

где  $code(ES_{a, C}^A)$  – описание СИК через состояние  $ES_{a, C}^A$ , обусловленное влиянием учитываемых типов ИВ. Т.к.  $code(ES_{a, C}^A)$  будет использоваться согласно  $T$ , представляется целесообразным потребовать раздельного описания различных составляющих СИК, т.е.

$$code(ES_{a, C}^A) = W_A, W_C, \quad (12)$$

где  $W_A$  и  $W_C$  – слова, кодирующие данные об антагонистическом (5) и коалиционном (7) ИК, соответственно.

Выделение из общего описания  $ES$  двух слов, кодирующих каждый соответствующий тип конфликтного ИВ, обосновано целью моделирования  $T$ . Содержание и структура слов  $W_A$  и  $W_C$  определяются

характеристиками потребителя информации –  $SM$  из (1). Например, для подсистемы управления ресурсами КРС, использующей логический вывод [9], словом целесообразно кодировать совокупность термов, каждый из которых есть высказывание об эмиссии, потенциальной или реализуемой одной из сторон ИК. При описании антагонистического ИВ для построения  $W_A$  с учетом (2) и (5) используются также термы – высказывания о рецепторах, способных своими алгоритмами реализовывать этапы (2) и (3) ИК. Такое содержание слов обеспечит подсистему управления ресурсами КРС информацией о природе существующих конфликтных ИВ, что позволит ей прогнозировать ИК [9]. При использовании же модели (12) для решения задачи о достаточности средств ЗИ, обеспечивающих конфиденциальность передаваемой по радиоканалу информации [8], слово  $W_A$  должно содержать термы, кодирующие данные о возможностях средств радиомониторинга и анализа его результатов. Далее для сохранения общности изложения абстрагируемся от конкретного содержания слов, кодирующих типы ИВ, и методов их получения.

С учетом введенного понятия индифферентного ИВ и (11) предлагается СИК описывать с помощью отображения

$$L_{K+} : ES \rightarrow code(ES_{a, C, I}^A), \\ code(ES_{a, C, I}^A) = W_A, W_C, W_I, \quad (13)$$

где  $W_I$  – слово, кодирующее данные об индифферентном ИВ.

Оценим информативность двух формализованных выше моделей СИК с привлечением методов теории информации. Для оценивания информативности описаний систем применяют алгоритмический, комбинаторный или вероятностный подходы [11]. С учетом цели работы и отсутствия вероятностного описания ИК, необходимого для вычисления энтропии Шеннона [16], оценивание информативности представляется адекватным только с алгоритмических позиций Колмогорова [11, 24].

В докладе [11] предложен подход к оцениванию информативности моделей ИК с использованием колмогоровской сложности как меры содержащейся в них информации. Колмогоровская сложность является эффективным инструментом для оценивания информативности описаний [24], т.к. является числовой характеристикой сложности описываемого объекта.

Алгоритмический подход ставит в соответствие количеству информации в слове  $x$  конечной длины простую колмогоровскую сложность ( $KS$ ) этого слова [24], определяемую как длина самого короткого описания  $у$  слова  $x$

$$KS^\Gamma(x) = \min\{l(y) | \Gamma(y) = x\},$$

где  $\Gamma$  – способ получения описания  $y$  слова  $x$ , представленный вычислимой функцией  $\Gamma(y)$ , определенной на множестве слов  $\{0,1\}^+$ ;  $l(y)$  – длина слова  $y$  при фиксированном  $\Gamma$ . В качестве  $x$  обычно рассматривается конечный объект, вследствие чего область значений функции  $\Gamma(y)$  определена природой описываемого объекта. Задание  $\Gamma(y) = x$  традиционно [24] предполагает наличие вычислимого кодирования.

Примем стандартное [24] допущение, что значения  $\Gamma(y)$  вычисляются соответствующим алгоритмом  $A_\Gamma$ , останавливающимся на заданном входе.

После пояснений содержания описаний  $code(ES_d^{A,C})$  и  $code(ES_d^{A,C,I})$  предлагается оценить ожидаемое повышение информативности модели СИК после введения в рассмотрение индифферентного ИВ.

Известны следующие соотношения, описывающие сложность описания отдельных слов и их наборов [11]:

$$KS(x_1, x_2) \leq KS(x_1) + KS(x_2) + O(\log_2 N),$$

$$KS(x_1, x_2, x_3) \leq KS(x_1) + KS(x_2) + KS(x_3) + O(\log_2 N),$$

где  $x_i, i = \overline{1,3}$  – слова длины не больше  $N$ ;  $O(\log_2 N)$  – сложность выбранного способа описания  $\Gamma$ . Тогда при использовании модели (12) сложности описаний  $ES_d$ , использующих единое, цельное описание радиоэлектронной обстановки и отдельное её описание через учитываемые типы ИВ, оцениваются выражением

$$KS(W_K) \leq KS(W_A) + KS(W_C) + O(\log_2 N), \quad (14)$$

а для модели СИК (13)

$$KS(W_{K+}) \leq KS(W_A) + KS(W_C) + KS(W_I) + O(\log_2 N), \quad (15)$$

где  $W_K = code(ES_d^{A,C})$  и  $W_{K+} = code(ES_d^{A,C,I})$  – описания СИК согласно принятым моделям при допущении, что слова  $W_A, W_C$  и  $W_I$  имеют длину не больше  $N$ .

С учетом содержания (14), (15) и того, что  $code(ES_d^{A,C})$  и  $code(ES_d^{A,C,I})$  являются разными описаниями объекта  $ES_d$ , справедливо

$$KS(W_A) + KS(W_C) + O(\log_2 N) < KS(W_A) + KS(W_C) + KS(W_I) + O(\log_2 N), \quad (16)$$

откуда следует, что разница в информативности моделей имеет значение

$$\Delta = KS(W_{K+}) - KS(W_K) = KS(W_I),$$

т.е. введение в рассмотрение еще одного типа ИВ обеспечивает повышение информативности на  $KS(W_I)$  битов при переходе от модели (12) к модели (13).

Вычисление колмогоровской сложности до этого осуществлялось при допущении независимости составляющих ИК между собой, т.е.

$$I(W_A:W_C) \approx I(W_C:W_I) \approx 0,$$

где  $I(W_A:W_C)$  – количество информации в слове  $W_A$  о слове  $W_C$ , вычисляемое как

$$I(W_A:W_C) = KS(W_C) - KS(W_C/W_A), \quad (17)$$

где  $KS(W_C/W_A)$  – условная сложность описания  $W_C$  при известном описании  $W_A$ , равная длине кратчайшего описания  $W_C$ .

При учете взаимных зависимостей  $K_A$  и  $K_C$ , что соответствует современным взглядам на ИК [16] с участием технологически развитых противников, получим по аналогии с (17) следующие соотношения:

$$I(W_C:W_A) = KS(W_A) - KS(W_A/W_C),$$

$$I(W_C:W_I) = KS(W_I) - KS(W_I/W_C),$$

$$I(W_A:W_I) = KS(W_I) - KS(W_I/W_A).$$

Последние выражения призваны описать взаимное влияние ИВ разных типов. Например, запись  $I(W_C:W_A)$  обозначает, что ИТС коалиции учитывают при формировании коалиционного ИВ особенности антагонистического ИВ и имеют одну из целей – адекватно реагировать на антагонистическое ИВ, которое, в свою очередь, обусловлено задачей эффективно действовать против коалиционного ИВ, что описывает величина  $I(W_A:W_C)$ . Величины же  $I(W_C:W_I)$  и  $I(W_A:W_I)$  характеризуют реакции коалиции и антагонистической стороны на индифферентное ИВ соответственно.

Тогда от выражений (14) и (15) перейдем к соответствующим формулам

$$KS(W_K) = I(W_C:W_A) + I(W_A:W_C),$$

$$KS(W_{K+}) = I(W_C:W_A) + I(W_A:W_C) + I(W_C:W_I) + I(W_A:W_I).$$

Из последних выражений по аналогии с (16) получим разницу в информативности моделей

$$\Delta = KS(W_{K+}) - KS(W_K) = I(W_C:W_I) + I(W_A:W_I).$$

Выражения для вычисления  $\Delta$  при различных допущениях о взаимном влиянии типов ИВ позволяют оценить повышение информативности описаний СИК при введении индифферентного ИВ в модель. Повышение информативности модели за счет введения в рассмотрение нового типа ИВ может быть объяснено такой аналогией, как увеличение количества информации об объекте анализа при увеличении числа сторон его рассмотрения, позволяющем учесть большее количество причинно-следственных связей.

Конкретное содержание алгоритма кодирования для получения слов  $W_A, W_C$  и  $W_I$  определяется архитектурой системы-потребителя информации, целями и правилами её функционирования, и выходит за рамки рассмотрения настоящей статьи.

Необходимо отметить, что для системы поддержки принятия решений по оцениванию достаточности средств ЗИ достаточно будет модели, в то время как для более эффективного управления ресурсами КРС



необходима конечная модель  $W_K = code(ES_d^{A,C})$ , которая ввиду необходимости учета взаимного влияния ИВ разных типов не может быть построена в реальном времени.

#### Выводы

Представленные результаты имеют как практическую значимость для исследования вопросов выбора средств ЗИ и построения конфликтно-устойчивых КРС РТК, так и теоретическую – могут быть полезны при исследовании ИК. Представленная модель СИК изначально предназначена для использования

в производственных системах [9], но может применяться и для других ИТС, функционирующих в условиях ИК. Усовершенствованная модель СИК обладает такими важными качествами, как адекватность, простота, проблемная ориентация, гибкость. Предложенный подход к оцениванию потенциальной информативной емкости моделей расширяет сферы применения теоретико-информационных методов. Развитие исследований будет посвящено доказательству необходимости и достаточности содержания модели ИК для выбора средств ЗИ в радиоканале РС РТК.

#### Литература

- Sharma P., Sarma K. K., Mastorakis N. E. Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications // IEEE Access. 2020. vol. 8, pp. 224761–224780. DOI: 10.1109/ACCESS.2020.3044453.
- Стародубцев Ю. И., Липатников В. А., Парфиров В. А. Проблема повышения разведывательной защищенности элементов военной системы связи // Военная мысль. 2023. № 7. С. 88–99.
- Головской В. А., Чернуха Ю. В., Семенюк Д. Б. Формализация задачи построения системы передачи данных робототехнического комплекса, функционирующего в условиях антагонистической киберэлектромагнитной деятельности // Вопросы кибербезопасности. 2019. № 6(34). С. 113–122. DOI: 10.21681/2311-3456-2019-6-113-122.
- Куракин А. С. Оценка эффективности функционирования группы беспилотных летательных аппаратов при выполнении задач аэрофотосъемки // Проблемы информационной безопасности. Компьютерные системы. 2024. № 1(58). С. 62–69. DOI: 10.48612/jisp/fpf1-59d2-x8t1.
- Борисов В. И., Вилков С. В. Технологическая платформа развития систем управления, связи и радиоэлектронной борьбы // Теория и техника радиосвязи. 2023. № 1. С. 5–11.
- Ельцов О. Н., Крутских П. П., Радзиевский В. Г. Конфликтная устойчивость роботизированных систем. – М.: Радиотехника, 2023. 350 с.
- Махов Д. С. Анализ некриптографических методов защиты информации в радиоканалах информационных систем // Вопросы кибербезопасности. 2024. № 1(59). С. 82–88. DOI: 10.21681/2311-3456-2024-1-82-88.
- Буторин Н. А., Головской В. А. Массовая проблема оценивания достаточности мер защиты информации // Прикладная математика: современные проблемы математики, информатики и моделирования: Материалы VI Всероссийской научно-практической конференции, Краснодар, 2024. – С. 169–173.
- Головской В. А. Операционная модель когнитивной радиосистемы робототехнического комплекса // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18. № 5. С. 12–20. DOI: 10.36724/2072-8735-2024-18-5-12-20.
- Козлитин С. Н., Козирацкий Ю. Л., Будников С. А. Моделирование совместного применения средств радиоэлектронной борьбы и огневого поражения в интересах повышения эффективности борьбы за превосходство в управлении // Системы управления, связи и безопасности. 2020. № 1. С. 49–73. DOI: 10.24411/2410-9916-2020-00001.
- Головской В. А. Расширение модели сложного радиоэлектронного конфликта // Радиолокация, навигация, связь: сборник трудов XXX Международной научно-технической конференции (г. Воронеж, 16–18 апреля 2024 г.), т. 5. С. 63–68.
- Сахнин А. А. Комплексная оценка радиоэлектронной защищенности военных систем связи. – М.: Радиотехника. 2022. 309 с.
- Михайлов Р. Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238–251. DOI: 10.24411/2410-9916-2020-10309.
- Андреев Г. И., Замарин М. Е., Созинов П. А., Тихомиров В. А. Концептуальная модель информационного взаимодействия радиоэлектронных средств // Радиотехника. 2021. Т. 85. № 12. С. 31–41. DOI: 10.18127/j00338486-202112-02.
- Власов В. В., Шевчук В. И., Шевчук Д. В., Ягольников С. В. Метод синтеза космической системы дистанционного зондирования Земли в условиях сложного информационного конфликта // Нейрокомпьютеры: разработка, применение. 2022. Т. 24. № 2. С. 30–34.
- Созинов П. А., Андреев Г. И., Тихомиров В. А., Замарин М. Е. Совместность производства энтропии с мерой оценки эффективности систем информационного обеспечения в радиоэлектронной борьбе // Радиотехника. 2023. Т. 87. № 5. С. 9–23. DOI: 10.18127/j00338486-202305-02.
- Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. – СПб.: Научное издание, 2020. 337 с.
- Антипин Б. М., Виноградов Е. М. Характеристики и параметры РЭС СПС, необходимые для анализа ЭМС в полосах совместного использования: аналитический обзор // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 6–18. DOI: 10.31854/1813-324X-2020-6-2-6-18.
- Михайлов Р. Л., Данилов Д. Ю., Потапов А. А., Гречко П. В. Динамическая координация подсистем наблюдения и воздействия: метод прогнозирования взаимодействий // Системы управления, связи и безопасности. 2024. № 3. С. 49–77. DOI: 10.24412/2410-9916-2024-3-049-077
- Антипова С. А., Воробьев А. А. Целенаправленная трансформация математических моделей на основе стратегической рефлексии // Компьютерные исследования и моделирование. 2019. Т. 11. № 5. С. 815–831. DOI: 10.20537/2076-7633-2019-11-5-815-831.
- Alfonseca M., Cebrian M., Anta A. F., Coviello L., Abeliuk A., Rahwan I. Superintelligence cannot be contained: lessons from computability theory // Journal of Artificial Intelligence Research. 2021. No 70. pp. 65–76. DOI: 10.1613/jair.1.12202.



22. Котенко И. В., Хмыров С. С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. 2022. № 4(50). 52–79. DOI: 10.21681/2311-3456-2022-4-52-79.
23. Грушо А. А., Грушо Н. А., Забейало М.И., Тимонина Е. Е., Шоргин С. Я. Сложные причинно-следственные связи // Информатика и ее применения. 2023. Т. 17. № 2. С. 84–89. DOI: 10.14357/19922264230212.
24. Верещагин Н. К., Семёнов А. Л., Шень А. Х. Последнее открытие Колмогорова? (Колмогоров и алгоритмическая статистика) // Теория вероятностей и ее применения. 2023. Т. 68. № 4. С. 719–750. DOI: 10.4213/tvp5650.

## A MODEL OF COMPLEX INFORMATION CONFLICT FOR ROBOTIC SYSTEMS

Golovskoy V. A.<sup>9</sup>

**Keywords:** algorithm, information conflict, information interaction, model, electronic conflict, Kolmogorov complexity, robotic complex.

**The purpose of the work** is to formalize the model of a complex information conflict and to constructively prove the increase in the informativeness of the model of such a conflict, improved by including indifferent information interaction in it.

**Research methods:** general scientific methods – abstraction, generalization, analysis, and methods of the theory of algorithms and information theory.

**The result of the study:** a well-known model of a complex information conflict of information technology systems has been formalized, its qualitative improvement has been carried out for the operating conditions of robotic complexes. It is proposed to measure the informativeness of formalized models directly, rather than indirectly, through modeling the influence of the models used on the quality of the system functioning. Using the abstractions of identification and potential feasibility, which are traditional for theoretical and algorithmic constructions, the approach to using Kolmogorov complexity for quantitative assessment of qualitative improvement of the considered model of complex information conflict is substantiated. Analytical expressions are obtained that allow evaluating the informativeness of the proposed models.

**Practical value:** the presented results provide an opportunity to solve the problems of assessing the sufficiency of information security tools and choosing a conflict-resistant state of the radio system, as well as expand the range of methods used in the study of information conflicts.

### References

1. Sharma P., Sarma K. K., Mastorakis N. E. Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications // IEEE Access, 2020. vol. 8, pp. 224761–224780. DOI: 10.1109/ACCESS.2020.3044453.
2. Starodubcev Yu. I., Lipatnikov V. A., Parfirov V. A. Problema povysheniya razvedyvatel'noj zashchishchennosti elementov voennoj sistemy svyazi // Voennaya mysl', 2023. No 7. pp. 88–99.
3. Golovskoy V. A., Chernuha Yu. V., Semenyuk D. B. Formalizatsiya zadachi postroeniya sistemy peredachi dannyh robototekhnicheskogo kompleksa, funkcioniruyushchego v usloviyah antagonistscheskoj kiberelektromagnitnoj deyatel'nosti // Voprosy kiberebezopasnosti [Cybersecurity issues], 2019, No 6 (34), pp. 113–122. DOI: 10.21681/2311-3456-2019-6-113-122.
4. Kurakin A. S. Ocenka effektivnosti funkcionirovaniya gruppy bespilotnyh letatel'nyh apparatov pri vypolnenii zadach aerofotos'emki // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy [Problems of information security. Computer systems], 2024, No 1(58). pp. 62–69. DOI: 10.48612/jisp/fpf1-59d2-x8t1.
5. Borisov V. I., Vilkov S. V. Tekhnologicheskaya platforma razvitiya sistem upravleniya, svyazi i radioelektronnoj bor'by // Teoriya i tekhnika radiosvyazi, 2023, No 1. pp. 5–11.
6. El'cov O. N., Krutskih P. P., Radzievskij V. G. Konfliktnaya ustojchivost' robotizirovannyh sistem. Moscow: Radiotekhnika, 2023. 350 p.
7. Makhov D. S. Analiz nekriptograficheskikh metodov zashchity informacii v radiokanalakh informacionnyh sistem // Voprosy kiberebezopasnosti [Cybersecurity issues], 2024. No 1(59). pp. 82–88. DOI: 10.21681/2311-3456-2024-1-82-88.
8. Butorin N. A., Golovskoy V. A. Massovaya problema ocenivaniya dostatochnosti mer zashchity informacii // Prikladnaya matematika: sovremennye problemy matematiki, informatiki i modelirovaniya: Materialy VI Vserossijskoj nauchno-prakticheskoy konferencii, Krasnodar, 2024. – pp. 169–173.
9. Golovskoy V. A. Operacionnaya model' kognitivnoj radiosistemy robototekhnicheskogo kompleksa // T-Comm: telekommunikacii i transport [T-Comm], 2024. vol. 18. No 5. pp. 12–20. DOI: 10.36724/2072-8735-2024-18-5-12-20.
10. Kozlitsin S. N., Kozirackij Yu. L., Budnikov S. A. Modelirovanie sovmestnogo primeneniya sredstv radioelektronnoj bor'by i ognevoogo porazheniya v interesah povysheniya effektivnosti bor'by za prevoskhodstvo v upravlenii // Sistemy upravleniya, svyazi i bezopasnosti [Systems of Control, Communication and Security], 2020. No 1. pp. 49–73. DOI: 10.24411/2410-9916-2020-00001.
11. Golovskoy V. A. Rasshirenie modeli slozhnogo radioelektronnoogo konflikta // Radiolokaciya, navigaciya, svyaz': sbornik trudov XXX Mezhdunarodnoj nauchno-tekhnicheskoy konferencii. Voronezh, vol. 5. pp. 63–68.
12. Sakhnin A. A. Kompleksnaya ocenka radioelektronnoj zashchishchennosti voennyh sistem svyazi. – Moscow, Radiotekhnika. 2022. 309 p.

<sup>9</sup> Vasilii A. Golovskoy, Ph.D. (in Engineering sciences), Associate Professor, Krasnodar Higher Military School named after army general S. M. Shtemenko, Krasnodar, Russia. E-mail: golovskoy\_va@mail.ru

13. Mikhailov R. L. Dinamicheskaya model' informacionnogo konflikta informacionno-telekommunikacionnyh sistem special'nogo naznacheniya // *Sistemy upravleniya, svyazi i bezopasnosti* [Systems of Control, Communication and Security], 2020. No 3. pp. 238–251. DOI: 10.24411/2410-9916-2020-10309.
14. Andreev G. I., Zamarin M. E., Sozinov P. A., Tikhomirov V. A. Konceptual'naya model' informacionnogo vzaimodejstviya radioelektronnyh sredstv // *Radiotekhnika* [Radioengineering], 2021. vol. 85. No 12. pp. 31–41 DOI: 10.18127/j00338486-202112-02.
15. Vlasov V. V., Shevchuk V. I., Shevchuk D. V., Yagol'nikov S. V. Metod sinteza kosmicheskoy sistemy distancionnogo zondirovaniya Zemli v usloviyah slozhnogo informacionnogo konflikta // *Nejrokompyutery: razrabotka, primenenie* [Neurocomputers], 2022. vol. 24. No 2. pp. 30–34.
16. Sozinov P. A., Andreev G. I., Tikhomirov V. A., Zamarin M. E. Sovmestnost' proizvodstva entropii s meroy ocenki effektivnosti sistem informacionnogo obespecheniya v radioelektronnoj bor'be // *Radiotekhnika* [Radioengineering], 2023. vol. 87. No 5. pp. 9–23. DOI: 10.18127/j00338486-202305-02.
17. Makarenko S. I. Modeli sistemy svyazi v usloviyah prednamerennyh destabiliziruyushchih vozdeystvij i vedeniya razvedki. – SPb.: High Tech Publishing House, 2020, 337 p.
18. Antipin B. M., Vinogradov E. M. Harakteristiki i parametry RES SPS, neobhodimye dlya analiza EMS v polosah sovmestnogo ispol'zovaniya: analiticheskij obzor // *Trudy uchebnyh zavedenij svyazi* [Proceedings of telecommunication universities], 2020. vol. 6. No 2. pp. 6–18. DOI: 10.31854/1813-324X-2020-6-2-6-18.
19. Mikhailov R. L., Danilov D. Yu., Potapov A. A., Grechko P. V. Dinamicheskaya koordinaciya podsystem nablyudeniya i vozdeystviya: metod prognozirovaniya vzaimodejstvij // *Sistemy upravleniya, svyazi i bezopasnosti* [Systems of Control, Communication and Security], 2024. No 3. pp. 49–77. DOI: 10.24412/2410-9916-2024-3-049-077
20. Antipova S. A., Vorob'ev A. A. Celenapravlenaya transformaciya matematicheskikh modelej na osnove strategicheskoy refleksii // *Kompyuternye issledovaniya i modelirovanie* [Computer Research and Modeling], 2019. vol. 11. No 5. pp. 815–831. DOI: 10.20537/2076-7633-2019-11-5-815-831.
21. Alfonseca M., Cebrian M., Anta A. F., Coviello L., Abeliuk A., Rahwan I. Superintelligence cannot be contained: lessons from computability theory // *Journal of Artificial Intelligence Research*, 2021. No 70. pp. 65–76. DOI: 10.1613/jair.1.12202.
22. Kotenko I. V., Khmyrov S. S. Analiz modelej i metodik, ispol'zuemyh dlya atribucii narushitelej kiberbezopasnosti pri realizacii celevyh atak // *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2022. No 4(50). pp. 52–79. DOI: 10.21681/2311-3456-2022-4-52-79.
23. Grusho A. A., Grusho N. A., Zabezhajlo M. I., Timonina E. E., Shorgin S. Ya. Slozhnye prichinno-sledstvennye svyazi // *Informatika i ee primeniya* [Informatics and applications], 2023. vol. 17. No 2. pp. 84–89. DOI: 10.14357/19922264230212.
24. Vereshchagin N. K., Semyonov A. L., SHen' A. H. Poslednee otkrytie Kolmogorova? (Kolmogorov i algoritmicheskaya statistika) // *Teoriya veroyatnostej i ee primeniya* [Theory of Probability and its Applications], 2023. vol. 68. No 4. pp. 719–750. DOI: 10.4213/tvp5650.

