АНАЛИЗ ПРОБЛЕМЫ ФОРМИРОВАНИЯ НАБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИОКАНАЛАХ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Головской В. А.[1]

DOI: 10.21681/2311-3456-2025-4-117-126

Цель работы *– провести анализ проблематики автоматизированного оценивания достаточности некриптографических средств защиты информации в радиоканалах радиосистем передачи данных робототехнических комплексов.*

Методы исследования: *общенаучные методы – анализ, дедуктивный вывод, методы системного анализа и теории алгоритмов, применение сопутствующих абстракций потенциальной реализуемости и актуальной бесконечности.*

Результат исследования: *предложен подход к формализации проблем в области информационной безопасности в виде конструктивных объектов, применение которого позволило сформировать соответствующие массовые проблемы защиты информации в радиоканалах радиосистем передачи данных робототехнических комплексов и оценить их на предмет алгоритмической разрешимости. Предложено использовать описание средств защиты информации через совокупность нетривиальных семантических свойств алгоритмов, ими управляющих. Данный подход обеспечивает возможность абстрагироваться от особенностей реализации средств защиты информации и использовать такие описания в составе конструктивных объектов при работе алгоритмов оценивания достаточности и выбора оптимального набора средств защиты информации в радиоканалах. Предложена гипотеза о взаимосвязи указанных массовых проблем, для проверки которой сформулирована и доказана теорема.*

Научная значимость: *представленные результаты формируют основания для исследования вычислительных аспектов задачи построения эффективного алгоритма формирования набора средств защиты информации в радиоканалах робототехнических комплексов. Предложенное описание средств защиты информации совокупностью нетривиальных семантических свойств управляющих ими алгоритмов обеспечивает возможность адекватного учета их сущностного содержания и значимых для решения задачи особенностей без необходимости рассмотрения их программной или аппаратно-программной реализации.*

Ключевые слова: *Алгоритм, алгоритмическая проблема, конфиденциальность, криптографическая защита информации, массовая проблема, машина Тьюринга, моделирование, угроза, проблема эквивалентности.*

Введение

В настоящее время требования практики к сокращению сроков разработки и поставки потребителю робототехнических комплексов (РТК) обострились критически. При этом, несмотря не существующие успехи в развитии теории и практики испытаний, наблюдаемые тенденции к увеличению функционала и интеллектуализации РТК обуславливают усложнение этапов проверки их заявленных свойств [1, 2]. Обусловленная указанными факторами проблема построения объяснимого искусственного интеллекта актуальна и для исследований вопросов защиты информации (ЗИ) [3]. Наличие подсистем криптографической ЗИ (КЗИ) в радиоканалах радиосистем передачи данных (РС) РТК обуславливает как снижение эффективной скорости передачи информации, так и увеличение массогабаритных характеристик робототехнических средств (РТС), сроков разработки таких РТК, как надсистемы, за счет необходимости проведения ряда обязательных исследований[2] и, соответственно, стоимости РТК. Также немаловажным моментом является необходимость выполнения ряда организационно-технических мероприятий при подготовке к применению РТК, содержащих подсистемы КЗИ, что в критических условиях является осложняющим фактором [4]. Указанные аспекты в совокупности с повышенным вниманием к безопасности информации в РТК [5, 6] актуализируют известную научно-техническую проблему [7–9] формирования оптимального набора средств ЗИ (СЗИ) в условиях ограниченности ресурсов. Дополнительную остроту этой проблеме придает существенное влияние человеческого фактора при оценивании угроз безопасности информации и принятии соответствующих решений на основании полученных оценок [10]. Так, методический документ[3] декларирует, что «независимо от результата формирования экспертной группы при оценке угроз безопасности информации существуют субъективные факторы,

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 Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Утверждено приказом ФСБ РФ от 9 февраля 2005 г. N 66.

3 Методический документ «Методика оценки угроз безопасности информации». Утвержден ФСТЭК России 5 февраля 2021 г.

связанные с психологией принятия решений. Это также может приводить как к занижению (ослаблению), так и к завышению (усилению) экспертами прогнозов и предположений при оценке угроз безопасности информации, что в свою очередь может привести к пропуску отдельных угроз безопасности информации или к неоправданным затратам на нейтрализацию неактуальных угроз».

Ввиду указанных выше аспектов вопрос о возможности обеспечения безопасности информации в радиоканалах не криптографическими СЗИ (НКСЗИ) инициирует исследования по анализу возможностей и синтезу НКСЗИ [3, 11–16], а также – по оцениванию их достаточности для обеспечения защищенности информации [9, 17–19].

Вопросы отнесения различных не криптографических средств обработки и преобразования информации и сигналов, ее переносящих, предназначенных для обеспечения конфиденциальности, целостности и доступности информации, к классу СЗИ являются дискуссионными [7, 17] ввиду важности дефиниции терминологического аппарата ЗИ, как и вопросы оценивания эффективности таких средств относительно ставших для ряда задач ЗИ традиционными криптографических методов [11]. При этом ввиду высокой практической значимости предметом многих исследований являются различные подходы, призванные обеспечить отдельные составляющие защищенности информации – конфиденциальность, целостность, доступность – в том числе, при передаче ее в радиоканалах [9, 11–20]. Необходимо отметить, что открытость разделяемого радиосистемами ресурса – радиочастотного спектра, который становится одновременно все более доступным для информационно-технических воздействий ввиду развития средств информационного противоборства, как интенсивного, так и экстенсивного, и все более загруженным [21], обостряет проблему защиты передаваемой по радиоканалам информации [7] в условиях антагонистического информационного конфликта.

Предлагаемая статья является развитием предложенной ранее [8] идеи построения алгоритма оценивания достаточности СЗИ и описания проблем ЗИ как конструктивных объектов со структурой, обусловленной предложенным для решения поставленной задачи теоретико-алгоритмическим подходом. Данный подход имеет достаточную историю[4] эффективного применения при исследованиях проблем информационной безопасности и обеспечивает возможность абстрагироваться от способа реализации анализируемых СЗИ.

4 Cohen F. Computational aspects of computer viruses // Computers & Security. – 1989. – Vol. 8, No. 4. P. 297–298.

1. Постановка задачи

Задача исследования возможностей создания конструктивного подхода и программы оценивания достаточности набора СЗИ в радиоканале, позволяющих минимизировать влияние субъективности экспертов, была предложена в [8]. Однако рассмотрение СЗИ при этом осуществлялось с позиций анализа лишь классов методов, составляющих функциональное наполнение СЗИ, а также остались нерассмотренными вопросы проверки гипотезы, доказательства необходимости и достаточности наборов входных данных и ряд других. В работе [21] была предложена модель антагонистического информационного конфликта и рассмотрено ее наполнение, в основном, данными о возможностях средств радиомониторинга и анализа его результатов, однако не был представлен анализ проблематики в широкой постановке и не определен перечень необходимых данных о РС РТК. Настоящая статья является промежуточным результатом исследования, имеющего цель – построение научно-методического аппарата формирования набора СЗИ, передаваемой по радиоканалам РС РТК. Цель статьи – провести анализ проблематики автоматизированного оценивания достаточности НКСЗИ в радиоканалах РС РТК. Объект исследования – функционирующая в условиях антагонистического информационного конфликта РС РТК, по радиоканалам которой передается подлежащая защите информация ограниченного распространения. Предмет исследования – обеспечение конфиденциальности информации, передаваемой в РС РТК по радиоканалам в условиях антагонистического информационного конфликта. Ограничение вопросов ЗИ только обеспечением ее конфиденциальности обусловлено сформировавшимися на практике актуальными угрозами безопасности информации, передаваемой по радиоканалам РС РТК определенного типа [4, 22].

Под РТК далее понимается автоматизированная система, являющаяся надсистемой для входящих в ее состав следующих подсистем [4, 21]: группа РТС, РС, сопряженная с системой ЗИ, включающей подсистему КЗИ, а также пункт управления. Рис. 1 призван проиллюстрировать принятую с учетом сформулированных объекта и предмета исследования декомпозицию РТК на подсистемы, осуществленную на логическом уровне.

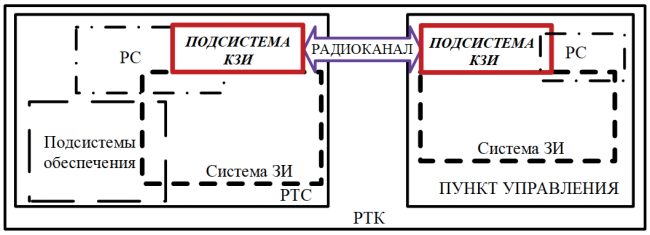

Рис. 1. Декомпозиция РТК на подсистемы

С учетом приведенных формальных элементов исследования сформулированы следующие ограничения:

- рассматривается применение средств КЗИ (СКЗИ) непосредственно и только для обеспечения конфиденциальности передаваемой в радиоканале информации, и не рассматриваются вопросы использования криптографических протоколов при аутентификации абонентов и прочие, формирующие актуальные уязвимости [4, 9, 23] в системе ЗИ;
- рассматриваются только вопросы разрешимости массовых проблем без анализа класса сложности разрешающего их алгоритма;
- по радиоканалам рассматриваемой РС передается только один вид информации, с одной меткой конфиденциальности;
- рассматривается наличие только внешнего нарушителя;
- не рассматриваются характеристики РТК, однако анализируемая проблематика наиболее актуальна для беспилотных летательных аппаратов.

К СКЗИ будем относить аппаратные, программные и аппаратно-программные средства, реализующие алгоритмы криптографического преобразования информации[5].

2. Формализация проблемы защиты информации в радиоканалах

Рассмотрим место проблемы обеспечения конфиденциальности информации среди множества традиционно рассматривающихся задач ЗИ.

С учетом цели работы используем методологию системного анализа, обеспечивающего адекватность предложений [8] по наполнению элементами проблематики ЗИ следующего известного[6] формализма, позволяющего построить модель M интересующего явления ISP:

$$M = \langle ISP, SM, T, IM, \Lambda \rangle, \quad (1)$$

где ISP – множество неформализованных проблем ЗИ, выступающих в качестве объекта-оригинала; SM – субъект моделирования, т.е. осуществляющая автоматизированное оценивание сущность, нуждающаяся в формальном описании проблемы ЗИ [8]; T – цель моделирования – обеспечение SM информацией, необходимой для формирования требуемого набора СЗИ [8]; IM – инфраструктура моделирования; Λ – язык описания, представляющий собой искомое отображение объекта в модель

$$\begin{cases} \Lambda: \Pi_k \longrightarrow P_k, \\ A_{SM}(P_k) = answer, \end{cases}$$

где $\Pi_k \in ISP$ – k-я неформализованная проблема ЗИ; $P_k = code(\Pi_k)$ – запись Π_k, обеспечивающая ее эффективную программную обработку за счет согласованности применяемых формализмов $code(\bullet)$ и A_{SM}; A_{SM} – алгоритм, используемый SM для вычисления формального ответа $answer$ о характеристиках требуемого набора СЗИ $W_h = [w_j, \ldots, w_p]$, обеспечивающего защищенность информации в P_k, $h = \overline{1, N_H}$, N_H – количество рассматриваемых СЗИ, $|W_h| \geq 1$.

Необходимо отметить, что цель моделирования T может иметь различные формулировки. Первоначальный запрос от практики был в обеспечении достаточности набора СЗИ [8], что будет соответствовать цели T_1. Однако первым автором работы [5] при обсуждении доклада [8] предложена иная формулировка цели, предполагающая формирование оптимального набора СЗИ, которой будет соответствовать T_2. При оптимизации набора СЗИ могут быть рассмотрены такие параметры СЗИ как пропускная способность, величина «накладных расходов» при шифровании, вычислительная эффективность, массогабаритные и температурные характеристики, стоимость и т.д. Далее будут последовательно рассмотрены проблемы, соответствующие обеим представленным формулировкам цели из (1).

В докладе [8] было предложено для анализа проблем ЗИ Π_k при конструировании Λ использовать теоретико-алгоритмический подход, характеризующийся формализацией любой массовой проблемы P_k конструктивным объектом – языком этой проблемы L_{P_k}, что позволило сформировать гипотезу об адекватности оценивания достаточности СЗИ согласно T_1 с позиций алгоритмической разрешимости массовых проблем P_k, соответствующих Π_k.

Под массовой или алгоритмической проблемой далее понимается класс однотипных задач, для которых необходимо найти единый разрешающий их алгоритм [2, 8]. Проблема P считается разрешимой в алгоритмическом смысле при существовании разрешающего ее язык $L_P = \{(data_j, decision_m)_k\}$ алгоритма $A_P(code(data_j)) = decision_m$, где $code(data_j) \in \Sigma^*$ обозначает непустое слово, кодирующее данные $data_j$ в алфавите Σ рассматриваемой машины Тьюринга (МТ) Θ_P, формализующей алгоритм A_P, или эквивалентного ей формализма. При этом A_P вычисляет слово $decision_m$, получив на вход $code(data_j)$.

Использование принятого теоретико-алгоритмического подхода позволяет с привлечением характерных для него абстракций при рассмотрении

5 МР 26.2.006-2021. Методические рекомендации «Информационная технология. Криптографическая защита информации. Термины и определения». Технический комитет по стандартизации ТК 26 «Криптографическая защита информации», М.: 2021 г. – 87 с.

6 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.

работающих по алгоритмам СЗИ пренебречь особенностями их реализации – аппаратная, программная или аппаратно-программная. Это обеспечивает адекватность представления СЗИ w_p как соответствующего набора нетривиальных семантических свойств алгоритма A_{w_p}, по которому функционирует w_p, т.е. отображение из (1) имеет вид $w_p \xrightarrow{\Lambda} \{s_r\}_p$, $r = \overline{1,N_R^p}$, где N_R^p – количество нетривиальных семантических свойств s_r, исчерпывающе описывающих алгоритм A_{w_p} функционирования СЗИ w_p. В общем случае предполагается, что для функционально различных СЗИ w_p, w_f и w_j мощности соответствующих множеств s_r не равны, т.е. $N_R^p \neq N_R^f \neq N_R^f$. Принято также допущение, что известны нетривиальные семантические свойства, соответствующие всем характеристикам анализируемых СЗИ и их наборам.

Использование предложенного отображения $w_p \xrightarrow{\Lambda} \{s_r\}_p$ позволяет повысить уровень конструктивности моделирования относительно [8] и сформулировать массовую проблему проверки задач, разрешаемых СКЗИ, на разрешимость их и НКСЗИ. С учетом сформулированного объекта исследования и содержания антагонистического информационного конфликта [21] массовую проблему P_S оценивания обеспечения защищенности информации в радиоканалах РС РТК опишем следующим языком:

$$L_S = \{(code(RS_i),code(D_j),code(ENW_q))_k, \\ code(W_h^l),dec_m\},\ n = \overline{1,N_K}, \quad (2)$$

где RS, $i = \overline{1,N_I}$ – модель i-й РС, реализующей передачу информации, подлежащей защите, между РТС по радиоканалу в условиях среды ENW_q, $q = \overline{1,\infty}$; D_j – достаточное описание угроз безопасности передаваемой по радиоканалу информации, инициируемых антагонистической стороной информационного конфликта, $j = \overline{1,N_D}$; W_h^l – набор используемых в RS_i СЗИ l-го класса, $l \in \{1,2\}$; $dec_m \in \{0,1\}$ – решение об эффективности набора СЗИ W_h^l в RS_i, $m = \overline{1,2}$. Рассматриваемые классы СЗИ – СКЗИ (К) при $l = 1$ и НКСЗИ (Ф) при $l = 2$ – не пересекаются при формировании набора СЗИ W_h^l, т.е. $\mathrm{K} \cap \Phi = \varnothing$.

Разрешимость массовой проблемы P_S с языком (2) означает потенциальное существование разрешающего ее алгоритма A_{L_S}, который для каждого набора $((code(RS_i),code(D_j),code(ENW_q))_k,code(W_h^l))$ дает бинарный ответ dec_m на вопрос об эффективности ЗИ, передаваемой в RS_i, с помощью набора СЗИ W_h^l при информационном конфликте с D_j в условиях ENW_q. Такая интерпретация P_S соответствует цели T_1. С учетом привлечения абстракций, принятых в теории алгоритмов, разрешающий L_S алгоритм описывается таким выражением:

$$A_{L_S}((code(RS_i),code(D_j),code(ENW_q))_k, \\ code(W_h^l)) = dec_m.$$

Представляется логичным связать с возможностью построения программы оценивания эффективности ЗИ в РС РТК следующее высказывание:

$$S^{IS} \Longleftrightarrow \exists A_{L_S}: A_{L_S}((code(RS_i),code(D_j),code(ENW_q))_k, \\ code(W_h^l)) = dec_m. \quad (3)$$

С учетом цели работы выделим из множества проблем (2), разрешаемых СКЗИ, т.е. при $l = 1$, собственное подмножество – класс проблем P_C обеспечения конфиденциальности передаваемой в RS_i информации, формализуемый языком L_C, что иллюстрирует рис. 2. Также выделен из $\mathrm{K} \cup \Phi$ подкласс СЗИ C, обеспечивающих ее конфиденциальность, т.е. $C \subseteq \{\mathrm{K},\Phi\}$. С учетом принятых при формировании (2) обозначений выделенное собственное подмножество $L_C \subseteq L_S$, представляющее особый интерес для настоящей работы, формализуемо языком следующей структуры:

$$L_C = \{(code(RS_i),code(D_j),code(ENW_q))_k, \\ code(C),dec_m\}. \quad (4)$$

$$L_C = \{(RS_i, D_j, ENW_q)_n, C, dec\}$$

$$L_S = \{(RS_i, D_j, ENW_q)_k, W_h^l, dec_m\}$$

Рис. 2. Вложенность массовых проблем ЗИ

С учетом вложенности $C \subseteq \{\mathrm{K},\Phi\}$ и $L_C \subseteq L_S$ очевидно, что при разрешимости проблемы L_S будет разрешимой и проблема L_C.

По аналогии с (3) свяжем с возможностью построения программы оценивания эффективности обеспечения применяемыми СЗИ конфиденциальности информации в радиоканале RS_i разрешимость массовой проблемы (4):

$$S^C \Longleftrightarrow \exists A_{L_C}: A_{L_C}((code(RS_i),code(D_j),code(ENW_q))_k, \\ code(C)) = dec_m, \quad (5)$$

где A_{L_C} – разрешающий L_C алгоритм.

Теория и практика показывают, что у множества L_C существует подмножество L_K, для которого конфиденциальность передаваемой информации обеспечивается СКЗИ. Тогда при разрешимости проблемы L_C будет разрешимой и ее подпроблема, формализуемая языком

$$L_K = \{(code(RS_i),code(D_j),code(ENW_q))_k, \\ code(K),1\}. \quad (6)$$

Выделим из $L_C \subseteq L_S$ подмножество проблем $L_\Phi \subseteq L_C$, разрешаемых НКСЗИ, т.е. содержащее такие наборы $(code(RS_i),code(D_j),code(ENW_q))_k = \alpha_k$, для которых

конфиденциальность передаваемой по радиоканалам RS_i информации обеспечивается при использовании набора СЗИ $W_h^{\Phi} \in \Phi$:

$$L_{\Phi} = \{\alpha_k, code(W_h^{\Phi}), 1\}, \quad (7)$$

где $j = \overline{1, N_{D_C}}$, N_{D_C} – количество детализированных моделей нарушителя, способного нарушить конфиденциальность передаваемой в радиоканале информации, $N_{D_C} < N_D$.

В работе [7] было показано и практика подтверждает, что существует подмножество проблем $P_{\text{КФ}} \subseteq P_C$, характеризующееся тем, что конфиденциальность передаваемой по радиоканалам RS_i информации обеспечивается, как СКЗИ, так и НКСЗИ, формализуемое

$$L_{\text{КФ}} = L_{\text{К}} \cap L_{\Phi}. \quad (8)$$

Рис. 3 иллюстрирует предлагаемое выделение подпроблем $L_{\text{К}}$, L_{Φ} и $L_{\text{КФ}}$ из массовой проблемы $L_C \subseteq L_S$. При разрешимости проблемы L_C будут разрешимыми проблемы $L_{\text{К}}$ и $L_{\text{КФ}}$ ввиду их вложенности в L_C. Однако разрешимость $L_{\text{КФ}}$ не может рассматриваться даже как необходимое условие для разрешимости L_C.

Теперь для рассмотрения возможности автоматизации оценивания достаточности СЗИ и выбора их подходящего набора $W_h^l \in \Phi$ проведем анализ проблемы, формализуемой языком (8), на предмет определения ее алгоритмической разрешимости. Известно, что при использовании дедуктивного подхода для автоматического построения решения задачи необходимым является доказательство существования ее решения.

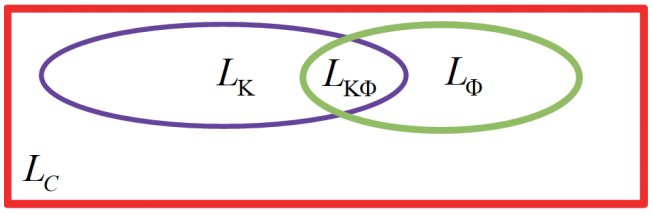

Рис. 3. Выделение подпроблем из массовой проблемы L_C

Разрешимость $L_{\text{КФ}}$ означает, что для любого набора α_k существует алгоритм $A_{L_{\text{КФ}}}(\alpha_k, \beta_h) = dec_m$, где $\beta_h = code(W_h^l)$, dec_m – ответ на вопрос об обеспечении конфиденциальности информации как с использованием СКЗИ ($W_h^{\text{К}}$), так и с использованием НКСЗИ (W_h^{Φ}). По аналогии с (3) и (5) с разрешимостью свяжем высказывание

$$S^{\text{КФ}} \Longleftrightarrow \exists A_{L_{\text{КФ}}} : A_{L_{\text{КФ}}}(\alpha_k, \beta_h) = dec_m. \quad (9)$$

С учетом алгоритмической природы β_h, как входа для предложенного $A_{L_{\text{КФ}}}$, очевидно, что истинность высказывания (9) согласована с разрешимостью вариации алгоритмической проблемы распознавания эквивалентности МТ. Необходимо отметить, что несмотря на известную неразрешимость ставшей классической массовой проблемы распознавания функциональной эквивалентности МТ, известны [24] варианты указанной проблемы, разрешимые за счет конкретизации вычислительной модели, содержания программы МТ и ее поведения.

Одним из направлений по конструированию разрешимых подпроблем неразрешимых массовых проблем является разрабатываемая в рамках генерического подхода [25] методология формирования такого подмножества множества входов, на элементах которого алгоритм остановится всегда. При этом за счет снижения требования массовости разрешающего алгоритма возможно обеспечение его приемлемой сложности. Однако сильная конкретизация делает проблему менее массовой, что обуславливает снижение ее интереса для практики. Отсюда возникают две задачи: определения условий баланса «массовость/разрешимость» и выбор наилучшей вычислительной модели. С учетом приведенных аргументов будем считать, что для массовой и интересной для практики версии (8) существует $A_{L_{\text{КФ}}}$, обеспечивающий истинность высказывания (9).

Рассмотрим алгоритмическую проблему, соответствующую цели T_2 из (1). В результате проведенного анализа сформулирована следующая **Гипотеза**: существование $A_{L_{\text{КФ}}}$ является необходимым условием существования алгоритма $A_{\Phi_C}(\alpha_k, B_c) = \beta_h^O$, разрешающего массовую проблему P_{Φ_C} определения оптимального набора СЗИ, формализуемую языком

$$L_{\Phi_C} = \{(\alpha_k, B_c)_y, \beta_h^O\},$$

где $B_c = \beta_0 \# \beta_1 \# \ldots \# \beta_{N_H - 1} \# \beta_{N_H}$, $\beta_h^O = code(\tilde{W}_h^l)$, $\tilde{W}_h^l \in \{W_h^l\}_{N_H}^{h=1}$ – оптимальный в определенном смысле набор СЗИ, # – служебный символ, предназначенный для разделения слов на ленте МТ. Свяжем с разрешимостью L_{Φ_C} высказывание

$$S^{\Phi_C} \Longleftrightarrow \exists A_{\Phi_C} : A_{\Phi_C}(\alpha_k, B_c) = \beta_h^O. \quad (10)$$

Для проверки гипотезы сформулирована **Теорема**: Взаимосвязь массовых проблем P_{Φ_C} и $P_{\text{КФ}}$ описывается высказыванием $S^{\Phi_C} \longrightarrow S^{\text{КФ}}$.

Доказательство. Для доказательства будем использовать широко применяемую в исследованиях массовых проблем [2, 8] технику сведения известной проблемы к исследуемой. Построены представленные на рис. 4а и 4б соответственно МТ $\Theta_{\text{КФ}}$, формализующая описанный выше алгоритм $A_{L_{\text{КФ}}}$, и ее модификация $\Theta_{\text{КФ}}^M$, заключающаяся в том, что $\Theta_{\text{КФ}}^M$ печатает только слова β_h, на которых $\Theta_{\text{КФ}}$ дает положительный ответ. Также построена представленная на рис. 4, в МТ Θ_{sort}, осуществляющая сортировку последовательности слов β_h в надслове

B_c по заданному параметру, соответствующему конкретной задаче оптимизации при цели T_2.

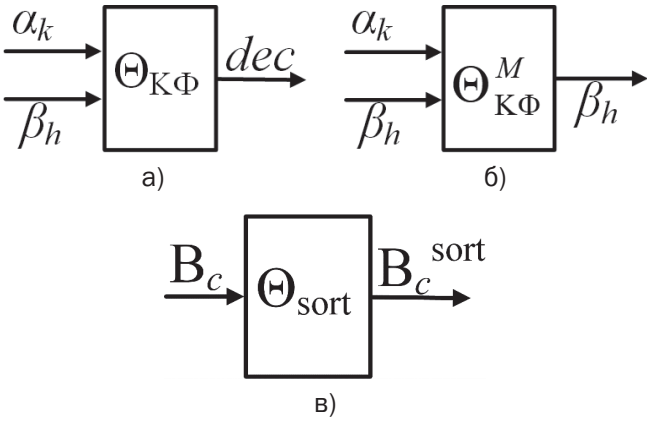

Рис. 4. Схемы машины Тьюринга, разрешающей проблему $L_{КФ}$ (а), ее модификация (б) и машины Тьюринга, разрешающей проблему сортировки (в)

Для доказательства теоремы построена схема сведения массовой проблемы $P_{КФ}$, приведенная на рис. 5, где между описанными МТ $\Theta^M_{КФ}$ и Θ_{sort} помещен буфер в виде ленты классической МТ, накапливающий все выходы $\Theta^M_{КФ}$. МТ Θ_{sort} начинает считывать с ленты надслово B_C только после останова $\Theta^M_{КФ}$, и, переработав B_C, печатает только слово β^O_h, соответствующее оптимальному набору СЗИ $\tilde{W}^l_h$. Очевидно, что ввиду известной разрешимости массовой проблемы сортировки из существования алгоритма $\Theta^M_{КФ}$ следует существование алгоритма A_{Φ_C} $(\alpha_k,B_c) = \beta^O_h$. Теорема доказана.

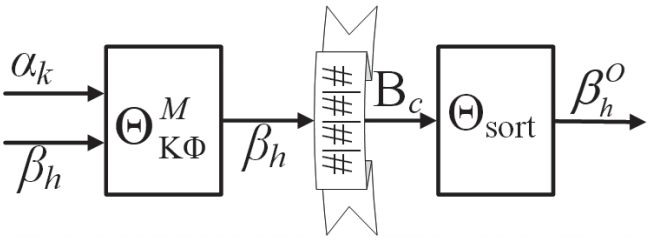

Рис. 5. Схема сведения $P_{КФ}$ к проблеме P_{Φ_C}

3. Обсуждение результатов

Алгоритм A_{Φ_C} позволит осуществлять интерпретируемое и объективно обоснованное формирование набора W^l_h СЗИ, обрабатываемой в РС РТК в условиях антагонистического информационного конфликта. Массовость в этом контексте будет означать инвариантность A_{Φ_C} к конкретному содержанию алгоритма функционирования СЗИ [2] и особенностям его реализации. В результате анализа содержания L_{Φ_C} сформулирована гипотеза об адекватности представления соответствующей проблемы P_{Φ_C} в терминах задачи о рюкзаке. Также важным фактором является правовая плоскость, и для практической разрешимости проблемы L_{Φ_C} представляется целесообразным нормативно определить новый тип информации, учитывающий зависимость от времени ее ценности и ограничения в распространении.

Сложность задачи построения эффективного алгоритма $A_{L_{КФ}}$, разрешающего интересную в практическом смысле соответствующую массовую проблему $P_{КФ}$, обуславливается необходимостью формирования требований к содержанию входа для $A_{L_{КФ}}$, поскольку эффективность любого алгоритма неразрывно связана с характеристиками входных для него данных [2]. При формировании требований к конкретному содержанию (α_k,β_h) должна быть обеспечена согласованность описаний RS_i, D_j, ENW_q и W^l_h еще до применения к ним операции $code(\bullet)$.

В работе [21] был предложен подход к наполнению D_j, ENW_q, однако наиболее сложным представляется вопрос конструирования Λ, обеспечивающего при описании W^l_h учет алгоритмом $A_{L_{КФ}}$ сущностного содержания НКСЗИ и криптографических СЗИ, имеющих подчас принципиальные различия, в том числе и на физическом уровне [7, 18]. Предложенный в настоящей работе подход к описанию СЗИ w_p набором нетривиальных семантических свойств $\{s_r\}_p$ алгоритма A_{w_p} позволит использовать в вычислениях в качестве исходных данных и криптоалгоритмы, как показано в работе[7], что полностью согласуется с возможностью построения алгоритмов над алгоритмами, обеспечиваемой формализмом МТ. Однако такой подход из-за принятой абстракции не будет учитывать некоторые особенности, обусловленные именно реализацией криптоалгоритмов в конкретных СКЗИ, что является при верификации криптографических протоколов недостатком [23], однако на данном этапе исследования считается приемлемым для решаемой задачи.

Рассмотрим некоторые предложенные ранее [8] требования к содержанию RS_i, которые призваны обеспечить согласованность с D_j и возможность построения интересной для практики применения РТК [4, 22] версии соответствующей массовой проблемы $P_{КФ}$. Раздельное описание РС РТК и обрабатываемой в ней информации, обусловленное необходимостью защиты именно информации (inf) в РС (rs), с учетом представленной детализации может быть формализовано на уровне грамматики как $RS_i = (rs\#inf)_i$. Малое, относительно других этапов жизненного цикла, время «активного существования» РТК в совокупности с высокой изменчивостью

7 Goldwasser S., Kalai Y. T., Popa R. A., Vaikuntanathan V., Zeldovich N. How to Run Turing Machines on Encrypted Data // Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, 2013. Vol. 8043. pp. 536–553, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40084-1_30

условий функционирования РТК обуславливают ограниченность времени [4], в течение которого информация в радиоканалах РС РТК может снять имеющуюся неопределенность и обеспечить эффективность выполнения задачи надсистемой, включающей РТК. Таким образом подтверждается тезис [8] о необходимости учета ценности информации в ее описании (inf), что может быть формализовано как $inf = object_v\#atr_f\#\gamma_l$, где $object_v$ – обозначение v-го объекта, данные о котором содержатся в inf, $v = \overline{1,N_V}$; atr_f – данные об атрибутах v-го объекта; γ_l – значения ценности информации inf, передаваемой по радиоканалам RS_i .

Необходимо отметить, что понятие ценности информации, введенное академиком А. А. Харкевичем[8] вместе с соответствующей мерой, активно используется в настоящее время при исследованиях различных научно-технических проблем [26, 27]. Ценность информации не является постоянной величиной в общем случае. Это косвенно подтверждает, как наличие процедур снижения грифа секретности и рассекречивания сведений, так и отнесение данных, считавшихся открытыми, к конфиденциальным.

С учетом приведенных выше аргументов для решения поставленной задачи необходимо построение вычислимой n-местной функции ценности информации $f^{\Gamma}(arg_1,\ldots,arg_n) = \gamma_l$, одним из аргументов которой является время t_2. Смещая акцент из области вычислимости функций в теоретико-алгоритмическую плоскость, последний тезис будет преобразован в задачу построения алгоритма $A_{\Gamma}(\alpha_k,t_z,\{arg_n\}) = \gamma_l$, разрешающего массовую проблему определения ценности информации в РС РТК, формализуемую языком $L_{\Gamma} = \{(\alpha_k,t_z,\{arg_n\})_x,\gamma_l\}$, $x = \overline{1,\infty}$, $n = \overline{1,N_N}$. Представленные предложения по учету ценности информации согласуется с положениями риск-ориентированного подхода [6].

8 Харкевич А. А. О ценности информации // Проблемы кибернетики, 1960. № 4. С. 53–57.

Выводы

Рассматриваемая проблема оценивания достаточности НКСЗИ обусловлена регуляторной политикой. В результате анализа проблемы осуществлена декомпозиция предварительно формализованной массовой проблемы оценивания достаточности СЗИ, передаваемой в радиоканалах РС РТК в условиях антагонистического информационного конфликта. Предложена и подтверждена гипотеза, имеющая как теоретическое, так и практическое значение.

Предложенное описание СЗИ совокупностью нетривиальных семантических свойств соответствующего алгоритма представляется адекватным для решаемой задачи, однако требует дальнейшего исследования.

Развитие результатов работы представляется целесообразным в следующих направлениях: исследование предложенного описания отображения $w_p \xrightarrow{\Lambda} \{s_r\}_p$ для корректной обработки результатов его применения; постановка задачи для T_2 в виде графовой модели, естественной для задачи о рюкзаке; определение необходимых и достаточных условий разрешимости L_{Φ_C} при разрешимости $L_{\text{КФ}}$; формирование интересной формулировки разрешимого L_{Γ} и конструирование эффективного алгоритма A_{Γ}.

Литература

1. Абросимов В. К. Принципы испытаний образцов вооружения, военной и специальной техники с реализацией технологии машинного обучения (полемические заметки) // Вооружение и экономика. 2024. № 2(68). С. 23–32.
2. Головской В. А. Анализ проблематики прогнозирования поведения когнитивных радиосистем // Радиотехника. 2024. Т. 88, № 12. С. 134–145.
3. Capuano N., Fenza G., Loia V., Stanzione C. Explainable Artificial Intelligence in CyberSecurity: A Survey // IEEE Access. 2022. vol. 10, pp. 93575–93600. DOI: 10.1109/ACCESS.2022.3204171.
4. Головской В. А., Винокуров А. В. Модель подсистемы выработки криптографических ключей системы защиты информации киберфизической системы // Известия ЮФУ. Технические науки. 2025. № 2 (244). С. 202–211. DOI: 10.18522/2311-3103-2025-2-202-211.
5. Pavlenko E. Y., Vasileva K. V., Lavrova D. S., Zegzhda D. P. Counteraction the cybersecurity threats of the in-vehicle local network // Journal of Computer Virology and Hacking Techniques. 2023. Vol. 19, No. 3. P. 399–408. DOI: 10.1007/s11416-022-00451-0.
6. Anagnostis I., Kotzanikolaou P., Douligeris C. Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services // IEEE Access. 2025. vol. 13. pp. 47955–47995. DOI: 10.1109/ACCESS.2025.3549861.
7. 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.
8. Головской В. А. Алгоритмические аспекты проблемы оценивания достаточности средств защиты информации // Перспективы безопасности – 2024: сборник материалов II НТК, посвященной информационной безопасности, Санкт-Петербург, 19–20 июня 2024 года. – Санкт-Петербург: ООО «Специальный Технологический Центр», 2024. С. 17–22.
9. Лэ В. Х., Комаров И. И., Привалов А. А., Пыркин А. А. Модель обеспечения непрерывности безопасного функционирования системы прослеживаемости качества продукции в условиях неустойчивой коммуникации // Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24. № 6. С. 949–961. DOI: 10.17586/2226-1494-2024-24-6-949-961.
10. Варенница В. В., Марков А. С., Савченко В. В., Цирлов В. Л. Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации // Вопросы кибербезопасности. 2021. № 5(45). С. 36–44. DOI: 10.21681/2311-3456-2021-5-36-44.

11. Pandey G. K., Gurjar D. S., Nguyen H. H, Yadav S. Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey // IEEE Access, 2022, vol. 10, pp. 112858–112897. DOI: 10.1109/ACCESS.2022.3215975.
12. Кукушкин С. С., Рубан Д. А., Козлов Е. В. Математическая модель и алгоритм формирования помехозащищённого сигнала синхронизации на основе использования составных кодовых конструкций псевдослучайных последовательностей // Двойные технологии. 2022. № 1(98). С. 40–45.
13. Глобин Ю. О., Финько О. А. Способ обеспечения имитоустойчивой передачи информации по каналам связи // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 2. С. 30–43. DOI: 10.36724/2409-5419-2020-12-2-30-43.
14. Басан Е. С., Прошкин Н. А., Силин О. И. Повышение защищенности беспроводных каналов связи для беспилотных летательных аппаратов за счет создания ложных информационных полей // Сибирский аэрокосмический журнал. 2022. Т. 23. № 4. С. 657–670. DOI: 10.31772/2712-8970-2022-23-4-657-670.
15. Tikhonov V., Taher A., Tikhonov S., Shulakova K., Hluschenko V., Chaika A. Turing Machine Development for High-Secure Data Link Encoding in the Internet of Things Channel // Proceedings of the 12th International Conference on Applied Innovations in IT (ICAIIT), 2024, Vol. 12, Iss. 1, pp. 1–10. DOI: 10.25673/1156354.
16. Gvozdeva I. G., Gromov A. S., Gvozdeva O. M. Development and implementation of the digital steganography method based on the embedding of pseudoinformation // Proceedings of the Institute for System Programming of the RAS. 2023. Vol. 35, No. 3. P. 63–70.
17. Белокопытов М. Л., Бянкин А. А., Алехин С. А. Способ защиты телеметрической информации при передаче в радиолиниях комплексов вооружения и военной техники // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 7-8(181-182). С. 81–87. DOI: 10.53816/23061456_2023_7-8_81.
18. Мальцев Г. Н., Матвеев С. А. Исследование защищенности системы командного радиоуправления подвижным объектом с использованием марковской модели преодоления нарушителем многоуровневой системы защиты информации // Труды Военно-космической академии имени А. Ф. Можайского. 2021. № 677. С. 153–163.
19. Ватрухин Е. М. Комплексная защита информации в каналах «земля-борт» // Вестник Концерна ВКО «Алмаз-Антей». 2020. № 4. С. 6–14. DOI: 10.38013/2542-0542-2020-4-6-14.
20. Манаенко С. С., Дворников С. В., Пшеничников А. В. Теоретические аспекты формирования сигнальных конструкций сложной структуры // Информатика и автоматизация. 2022. Т. 21, № 1. С. 68–94. DOI: 10.15622/ia.2022.21.3.
21. Головской В. А. Модель сложного информационного конфликта для робототехнических комплексов // Вопросы кибербезопасности. 2025. № 1 (65). С. 86–95. DOI: 10.21681/2311-3456-2025-1-86-95.
22. Бирюков П. А., Тимохин А. А., Макаренко С. И. Бригады сухопутных войск, вооруженные беспилотными летательными аппаратами: обоснование создания, предложения по их структуре, способам боевого применения и техническому обеспечению с учетом опыта специальной военной операции на Украине // Системы управления, связи и безопасности. 2024. № 2. С. 43–70. DOI: 10.24412/2410-9916-2024-2-043-070.
23. Бабенко Л. К., Писарев И. А. Язык PDA для динамического анализа криптографических протоколов // Вопросы кибербезопасности. 2020. № 5(39). С. 19–29. DOI: 10.21681/2311-3456-2020-05-19-29.
24. Zakharov V. A. Efficient Equivalence Checking Technique for Some Classes of Finite-State Machines // Automatic Control and Computer Sciences. 2021. Vol. 55, pp. 670–701. DOI: 10.3103/S014641162107018X.
25. Рыбалов А. Н. Генерически неразрешимые и трудноразрешимые проблемы // Прикладная дискретная математика. 2024. № 63. С. 109–116. DOI: 10.17223/20710410/63/7.
26. Чечин И. В., Маринин А. А., Новиков П. А., Диченко С. А., Самойленко Д. В. Комбинационное кодирование данных с учетом анализа ценности содержащейся информации // Проблемы информационной безопасности. Компьютерные системы. 2023. № 4(57). С. 31–41. DOI: 10.48612/jisp/mvrb-h5xa-xx1r.
27. Копкин Е. В., Деев В. В. Алгоритм построения оптимальной диагностической процедуры по показателю ценности информации на основе принципа максимума Понтрягина // Информация и космос. 2024. № 1. С. 65–72.

ANALYSIS OF THE PROBLEM OF FORMING A SET OF INFORMATION SECURITY TOOLS IN THE RADIO CHANNELS OF ROBOTIC COMPLEXES

Golovskoy V. A.[9]

Keywords: *algorithm, algorithmic problem, confidentiality, cryptographic protection of information, mass problems, Turing machine, simulation, threat, equivalence problems.*

The purpose of the work *is to analyze the problems of automated assessment of the sufficiency of non-cryptographic information security tools in radio channels of radio data transmission systems of robotic complexes.*

Research methods*: general scientific methods – analysis, deductive inference, methods of system analysis and theory of algorithms, application of related abstractions of potential realizability and actual infinity.*

The result of the study: *an approach to formalizing problems in the field of information security in the form of constructive objects is proposed, the application of which made it possible to form the corresponding massive problems*

9 Golovskoy Vasiliy Andreevich, 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

of information protection in radio channels of radio data transmission systems of robotic complexes and evaluate them for algorithmic solvability. It is proposed to use the description of information security tools through a set of non-trivial semantic properties of the algorithms that control them. This approach provides an opportunity to abstract from the specifics of the implementation of information security tools and use such descriptions as part of constructive objects when using algorithms for assessing sufficiency and choosing the optimal set of information protection tools in radio channels. A hypothesis about the interrelation of these mass problems is proposed, for which a theorem is formulated and proved.

Scientific significance: *the presented results form the basis for the study of computational aspects of the task of constructing an effective algorithm for the formation of a set of information security tools in the radio channels of robotic complexes. The proposed description of information security tools by a set of non-trivial semantic properties of the algorithms controlling them provides the possibility of adequate consideration of their essential content and features significant for solving the problem without the need to consider their software or hardware-software implementation.*

References

1. Abrosimov V. K. Principy ispytanij obrazcov vooruzhenija, voennoj i special'noj tehniki s realizaciej tehnologii mashinnogo obuchenija (polemicheskie zametki) // Vooruzhenie i jekonomika. 2024. № 2(68). S. 23–32.
2. Golovskoj V. A. Analiz problematiki prognozirovanija povedenija kognitivnyh radiosistem // Radiotehnika. 2024. T. 88, № 12. S. 134–145.
3. Capuano N., Fenza G., Loia V., Stanzione C. Explainable Artificial Intelligence in CyberSecurity: A Survey // IEEE Access. 2022. vol. 10, pp. 93575–93600. DOI: 10.1109/ACCESS.2022.3204171.
4. Golovskoj V. A., Vinokurov A. V. Model' podsistemy vyrabotki kriptograficheskih kljuchej sistemy zashhity informacii kiberfizicheskoj sistemy // Izvestija JuFU. Tehnicheskie nauki. 2025. № 2 (244). S. 202–211. DOI: 10.18522/2311-3103-2025-2-202-211.
5. Pavlenko E. Y., Vasileva K. V., Lavrova D. S., Zegzhda D. P. Counteraction the cybersecurity threats of the in-vehicle local network // Journal of Computer Virology and Hacking Techniques. 2023. Vol. 19, No. 3. P. 399–408. DOI: 10.1007/s11416-022-00451-0.
6. Anagnostis I., Kotzanikolaou P., Douligeris C. Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services // IEEE Access. 2025. vol. 13. pp. 47955–47995. DOI: 10.1109/ACCESS.2025.3549861.
7. Mahov D. S. Analiz nekriptograficheskih metodov zashhity informacii v radiokanalah informacionnyh sistem // Voprosy kiberbezopasnosti. 2024. № 1(59). S. 82–88. DOI: 10.21681/2311-3456-2024-1-82-88.
8. Golovskoj V. A. Algoritmicheskie aspekty problemy ocenivanija dostatochnosti sredstv zashhity informacii // Perspektivy bezopasnosti – 2024: sbornik materialov II NTK, posvjashhennoj informacionnoj bezopasnosti, Sankt-Peterburg, 19–20 ijunja 2024 goda. – Sankt-Peterburg: OOO «Special'nyj Tehnologicheskij Centr», 2024. S. 17–22.
9. Lje V. H., Komarov I. I., Privalov A. A., Pyrkin A. A. Model' obespechenija nepreryvnosti bezopasnogo funkcionirovanija sistemy proslezhivaemosti kachestva produkcii v uslovijah neustojchivoj kommunikacii // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2024. T. 24. № 6. S. 949–961. DOI: 10.17586/2226-1494-2024-24-6-949-961.
10. Varenica V. V., Markov A. S., Savchenko V. V., Cirlov V. L. Prakticheskie aspekty vyjavlenija ujazvimostej pri provedenii sertifikacionnyh ispytanij programmnyh sredstv zashhity informacii // Voprosy kiberbezopasnosti. 2021. № 5(45). S. 36–44. DOI: 10.21681/2311-3456-2021-5-36-44.
11. Pandey G. K., Gurjar D. S., Nguyen H. H, Yadav S. Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey // IEEE Access, 2022, vol. 10, pp. 112858–112897. DOI: 10.1109/ACCESS.2022.3215975.
12. Kukushkin S. S., Ruban D. A., Kozlov E. V. Matematicheskaja model' i algoritm formirovanija pomehozashhishhjonnogo signala sinhronizacii na osnove ispol'zovanija sostavnyh kodovyh konstrukcij psevdosluchajnyh posledovatel'nostej // Dvojnye tehnologii. 2022. № 1(98). S. 40–45.
13. Globin Ju. O., Fin'ko O. A. Sposob obespechenija imitoustojchivoj peredachi informacii po kanalam svjazi // Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli. 2020. T. 12. № 2. S. 30–43. DOI: 10.36724/2409-5419-2020-12-2-30-43.
14. Basan E. S., Proshkin N. A., Silin O. I. Povyshenie zashhishhennosti besprovodnyh kanalov svjazi dlja bespilotnyh letatel'nyh apparatov za schet sozdanija lozhnyh informacionnyh polej // Sibirskij ajerokosmicheskij zhurnal. 2022. T. 23. № 4. S. 657–670. DOI: 10.31772/2712-8970-2022-23-4-657-670.
15. Tikhonov V., Taher A., Tikhonov S., Shulakova K., Hluschenko V., Chaika A. Turing Machine Development for High-Secure Data Link Encoding in the Internet of Things Channel // Proceedings of the 12th International Conference on Applied Innovations in IT (ICAIIT), 2024, Vol. 12, Iss. 1, pp. 1–10. DOI: 10.25673/1156354.
16. Gvozdeva I. G., Gromov A. S., Gvozdeva O. M. Development and implementation of the digital steganography method based on the embedding of pseudoinformation // Proceedings of the Institute for System Programming of the RAS. 2023. Vol. 35, No. 3. P. 63–70.
17. Belokopytov M. L., Bjankin A. A., Alehin S. A. Sposob zashhity telemetricheskoj informacii pri peredache v radiolinijah kompleksov vooruzhenija i voennoj tehniki // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. 2023. № 7-8(181-182). S. 81–87. DOI: 10.53816/23061456_2023_7-8_81.
18. Mal'cev G. N., Matveev S. A. Issledovanie zashhishhennosti sistemy komandnogo radioupravlenija podvizhnym ob#ektom s ispol'zovaniem markovskoj modeli preodolenija narushitelem mnogourovnevoj sistemy zashhity informacii // Trudy Voenno-kosmicheskoj akademii imeni A. F. Mozhajskogo. 2021. № 677. S. 153–163.
19. Vatruhin E. M. Kompleksnaja zashhita informacii v kanalah «zemlja-bort» // Vestnik Koncerna VKO «Almaz-Antej». 2020. № 4. S. 6–14. DOI: 10.38013/2542-0542-2020-4-6-14.
20. Manaenko S. S., Dvornikov S. V., Pshenichnikov A. V. Teoreticheskie aspekty formirovanija signal'nyh konstrukcij slozhnoj struktury // Informatika i avtomatizacija. 2022. T. 21, № 1. S. 68–94. DOI: 10.15622/ia.2022.21.3.
21. Golovskoj V. A. Model' slozhnogo informacionnogo konflikta dlja robototehnicheskih kompleksov // Voprosy kiberbezopasnosti. 2025. № 1 (65). S. 86–95. DOI: 10.21681/2311-3456-2025-1-86-95.

22. Birjukov P. A., Timohin A. A., Makarenko S. I. Brigady suhoputnyh vojsk, vooruzhennye bespilotnymi letatel'nymi apparatami: obosnovanie sozdanija, predlozhenija po ih strukture, sposobam boevogo primenenija i tehnicheskomu obespecheniju s uchetom opyta special'noj voennoj operacii na Ukraine // Sistemy upravlenija, svjazi i bezopasnosti. 2024. № 2. S. 43–70. DOI: 10.24412/2410-9916-2024-2-043-070.
23. Babenko L. K., Pisarev I. A. Jazyk PDA dlja dinamicheskogo analiza kriptograficheskih protokolov // Voprosy kiberbezopasnosti. 2020. № 5(39). S. 19–29. DOI: 10.21681/2311-3456-2020-05-19-29.
24. Zakharov V. A. Efficient Equivalence Checking Technique for Some Classes of Finite-State Machines // Automatic Control and Computer Sciences. 2021. Vol. 55, pp. 670–701. DOI: 10.3103/S014641162107018X.
25. Rybalov A. N. Generic heski nerazreshimye i trudnorazreshimye problemy // Prikladnaja diskretnaja matematika. 2024. № 63. S. 109–116. DOI: 10.17223/20710410/63/7.
26. Chechin I. V., Marinin A. A., Novikov P. A., Dichenko S. A., Samojlenko D. V. Kombinacionnoe kodirovanie dannyh s uchetom analiza cennosti soderzhashhejsja informacii // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023. № 4(57). S. 31–41. DOI: 10.48612/jisp/mvrb-h5xa-xx1r.
27. Kopkin E. V., Deev V. V. Algoritm postroenija optimal'noj diagnosticheskoj procedury po pokazatelju cennosti informacii na osnove principa maksimuma Pontrjagina // Informacija i kosmos. 2024. № 1. S. 65–72.