Раздел III. Связь, навигация и наведение

УДК 621.391.81:004.056.55:004.89 DOI 10.18522/2311-3103-2025-2-202-211

В.А. Головской, А.В. Винокуров

МОДЕЛЬ ПОДСИСТЕМЫ ВЫРАБОТКИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ

Исследование посвящено совершенствованию подсистемы защиты информации в радиоканалах киберфизической системы на примере робототехнического комплекса (РТК). Рассмотрены современные и перспективные критические условия применения РТК, обуславливающие наборы требований к характеристикам как РТК, так и их подсистем, таким как радиосистема передачи данных (РС) и подсистема защиты информации. Одним из подходов к выполнению требований является унификация указанных подсистем РТК, которая может быть разделена условно на две научно-технические задачи: унификация радиопротоколов и унификация средств защиты информации в радиоканалах РС. В работе представлены полученные в результате анализа практические проблемы, лежащие на пересечении двух областей исследования – РС и подсистем защиты информации. Сформулирована гипотеза о потенциальной возможности эффективного разрешения одной из указанных практических проблем – обеспечения системы защиты информации криптографическими ключами – путем включения в систему защиты информации РТК подсистемы выработки криптографических ключей (ПВКК) из используемых в качестве исходной ключевой информации биометрических данных. Предлагаемое усовершенствование имеет несколько аспектов – нормативный, экономический, технический. В работе исследуется только научно-техническая сторона вопроса, в результате чего предложена функциональная модель ПВКК. Целью работы является разработка модели функционирования ПВКК для системы криптографической защиты информации в радиоканалах РС РТК и формирование её алгоритмического наполнения. Объект исследования – система криптографической защиты информации в радиоканалах РС. Предмет исследований – алгоритм выработки криптографических ключей для системы криптографической защиты информации в радиоканалах РС РТК. Для достижения цели обоснован класс привлекаемых абстракций и методический аппарат, использующий положения теории алгоритмов для доказательства существования алгоритма, разрешающего сформулированную массовую проблему и обладающего заданными нетривиальными семантическими свойствами. Методы исследования – анализ, аналогия, синтез, декомпозиция, абстрагирование. Сформулирована основная массовая проблема и гипотеза о её разрешимости. С целью проверки гипотезы сформулирована и доказана соответствующая теорема. Предложенная модель обеспечивает исследования возможностей моделируемой подсистемы по реализации сформулированных принципов функционирования и позволяет доказывать совместную эффективную реализуемость различных алгоритмов обработки информации.

Алгоритм; безопасность информации; биометрические данные; биометрия; защита информации; информационный конфликт; киберфизическая система; криптографический ключ; массовая проблема; модель; радиосистема; робототехнический комплекс.

V.A. Golovskoy, A.V. Vinokurov

A MODEL OF A SUBSYSTEM FOR GENERATING CRYPTOGRAPHIC KEYS OF THE CYBERPHYSICAL SYSTEM INFORMATION PROTECTION SYSTEM

The study is devoted to improving the subsystem of information protection in the radio channels of a cyberphysical system using the example of a robotic complex (RTC). Modern and promising critical conditions for the use of RTCs are considered, which determine the sets of requirements for the characteristics of both RTCs and their subsystems, such as the radio data transmission system (RS) and the information security subsystem. One of the approaches to meeting the requirements is the unification of these

RTC subsystems, which can be divided conditionally into two scientific and technical tasks: unification of radio protocols and unification of information security tools in RS radio channels. The paper presents the practical problems obtained as a result of the analysis, which lie at the intersection of two areas of research – RS and information security subsystems. A hypothesis has been formed about the potential for effective resolution of one of these practical problems – providing an information protection system with cryptographic keys - by including a cryptographic key generation subsystem (CKGS) from biometric data used as the initial key information in the RTC information protection system. The proposed improvement has several aspects – regulatory, economic, and technical. The paper examines only the scientific and technical side of the issue, as a result of which a functional model of the CKGS is proposed, which provides a study of the possibilities of the modeled subsystem for the implementation of the formulated principles of functioning. The purpose of the work is to develop a model of the CKGS functioning for the cryptographic information protection system in the RS RTC radio channels and the formation of its algorithmic content. The object of research is a system of cryptographic information protection in RS radio channels. The subject of the research is an algorithm for generating cryptographic keys for a cryptographic information protection system in RS RTC radio channels. To achieve this goal, a class of abstractions involved and a methodological apparatus are substantiated that uses the provisions of the theory of algorithms to prove the existence of an algorithm that solves a formulated mass problem and has specified non-trivial semantic properties. Research methods – analysis, analogy, synthesis, decomposition, abstraction. The main mass problem and the hypothesis of its solvability are formulated. In order to test the hypothesis, the corresponding theorem is formulated and proved. The proposed model makes it possible to prove the joint effective feasibility of various information processing algorithms.

Algorithm; information security; biometric data; biometrics; information protection; information conflict; cyberphysical system; cryptographic key; mass problem; model; radio system; robotics complex.

Введение. Возросшая доступность вычислительных возможностей обусловила наблюдаемый в настоящее время резкий рост количества сфер применения автономных технических систем и являющихся их развитием интеллектуальных киберфизических систем (КФС) [1–3]. Примером КФС могут служить интеллектуальные транспортные системы [4] или робототехнические комплексы (РТК) [3, 5], функционирующие в критических условиях или с прогнозируемо критическими последствиями. Развитие способностей КФС обусловило прогресс в конструировании техник атак на их информационные ресурсы [6]. В случае, когда указанные выше системы относятся к системам реального времени, появляются новые задачи в обеспечении информационной безопасности их ресурсов [7], что дополнительно осложняется жесткими требованиями к массо-габаритным и энергетическим характеристикам КФС и их подсистем.

Дополнительную остроту проблеме защиты информации в КФС придает тенденция к расширению спектра задач, выполняемых представителем их класса – РТК. Анализ литературы [8–10] и практика позволяют констатировать, что в настоящее время имеют место следующие особенности разработки РТК:

- технологическое несовершенство предприятий промышленности РФ, проявляющаяся, в том числе, в ограниченности номенклатуры и характеристиках выпускаемых вычислительных средств и телекоммуникационного оборудования;
- наличие жестких ресурсных ограничений (энергетических, структурных и др.), обусловленных требуемой автономностью РТК;
- высокая степень интеграции ресурсов РТК;
- ужесточение требований практики по сокращению сроков разработки РТК и поставки их конечному пользователю;
- пересмотр подходов к содержанию и длительности этапов жизненного цикла РТК – эксплуатация может длиться ничтожное время относительно прочих этапов.

Последний фактор в совокупности с условиями эксплуатации обуславливают необходимость пересмотра [10, 11] существующих подходов к формированию требований к подсистемам РТК, в частности – к подсистеме защиты информации. Указанная необходимость является одним из аспектов проблемы унификации разрозненных радиосистем передачи данных (РС) РТК [10, 11], являющейся известной и актуальной не только применительно к радиосистемам [12]. При этом решение проблемы унификации должно обеспечить построение единой, но гибкой и модульной эффективной РС РТК.

Постановка задачи. Несмотря на наличие системы взглядов на разработку специальной техники, приведенные выше аргументы, результаты исследований [10–14] и практика обуславливают следующие аспекты, вынуждающие рассматривать вопросы информационной безопасности ресурсов РТК с новых позиций:

требование минимизации стоимости подсистем РТК;

- требование наличия штатной схемы автономного уничтожения носителей информации и целых подсистем защиты информации;
- малое время, в течение которого подлежащая защите информация, циркулирующая в радиоканалах РС, является ценной;
- возникновение новых угроз, таких как атаки на модели обучения;
- наличие проблемы обеспечения средств криптографической защиты информации (СКЗИ) криптографическими ключами (КК).

Последняя проблема, являющаяся известной [15] и сугубо практической, обострилась в последние годы в связи с увеличением доли РТК, в радиоканалах РС которых информация подлежит защите, и их особенностями функционирования, не обеспечивающими возможность получить и использовать новые КК взамен скомпрометированных или с истекшим сроком действия. Под КК согласно [16] понимается совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Рассмотренные выше факторы обуславливают принятую в настоящей статье степень детализации РТК, из которого выделен объект исследования – система криптографической защиты информации (КЗИ) в радиоканалах РС. Под РТК в работе понимается КФС, состоящая из следующих подсистем:

- группа робототехнических средств (РТС);
- РС и подсистемы обеспечения, выделяемые на логическом уровне.

При наличии в составе РТК пункта управления, реализующего функции обработки информации и управления РТС оператором, такой РТК будет относиться к социокиберфизическим системам [17].

Из множества направлений исследований в области КЗИ для обозначенного объекта исследований наиболее актуальны следующие:

- низкоресурсная криптография [18];
- обеспечение стойкости криптоалгоритмов при минимизации длины КК [15];
- личностное шифрование [19].

Вопросы низкоресурсной криптографии и минимизации длины КК активно исследуются ввиду бурного развития развития облачных технологий и интернета вещей [13, 18, 20, 21]. Лежащая в основе личностного шифрования идея использования биометрических данных (БмД) для применения в системах КЗИ не нова [22], однако в лишь недавно на практике стала возможна реализация ее с требуемым качеством [18, 21], ввиду чего БмД рассматриваются как источник уникальных данных для решения различных практических задач [19, 23-27], в том числе задач защиты информации. Важным вопросом в современной криптографии является выбор алгоритмической проблемы [28] для формирования на ее основании КК. В работе [19] был предложен протокол личностного шифрования, предполагающий формирование КК для асимметричной криптосистемы из БмД, а также проведен его анализ с позиций безопасности. Однако применение асимметричных криптосистем для рассматриваемого класса КФС не может быть осуществлено по ряду известных причин. Анализ приведенных выше проблем, особенностей и аргументов позволил сформулировать гипотезу: алгоритмическая проблема разрешимости множества точек, являющегося отображением конкретного набора БмД операторов социокиберфизических систем, может быть использована как основание для построения подсистемы выработки КК (ПВКК) для системы КЗИ унифицированной РС РТК.

Настоящая статья является продолжением исследований по формированию системы подходов к построению унифицированной РС РТК [9, 11], и имеет целью разработать модель функционирования ПВКК для системы КЗИ в радиоканалах РС РТК и сформировать её алгоритмическое наполнение. В качестве предмета исследований определен алгоритм выработки КК для системы КЗИ в радиоканалах РС РТК.

С учетом приведенных формальных элементов исследования сформулированы следующие ограничения, позволяющие абстрагироваться от некоторых важных проблем обеспечения ИБ ресурсов РТК, являющихся предметом других исследований [10, 11, 29]:

- рассматривается применение СКЗИ непосредственно и только для обеспечения конфиденциальности передаваемой в радиоканалах информации;
- не рассматриваются вопросы аутентификации абонентов, разграничения прав доступа и прочие;
- по радиоканалам передается информация, не содержащая сведений, составляющих государственную тайну;
- рассматривается наличие только внешнего нарушителя;
- акцент делается на научно-технических аспектах проблемы, и не берутся во внимание правовые, обусловленные существующими требованиями регуляторов.

Формирование модели. Предлагается к рассмотрению разработанная функциональная модель ПВКК, формализованная с использованием нотации IDEF0. Рис. 1 иллюстрирует первый уровень описания функциональной модели ПВКК. В качестве входа предлагается рассматривать набор символов $f_i \in F$, являющийся инъективным отображением набора БмД выбранного субъекта.

Управление реализуется на основе:

- введенного ранее множества образов F, являющихся отображением БмД;
- требований к информативным наборам признаков P;
- требований к набору тестов на случайность R;
- требуемой длины КК L. При это предполагается, что подсистема КЗИ поддерживает возможность изменять по требованию размер КК, что обеспечит возможность генерирования КК для различных типов СКЗИ.

Рис. 1. Функциональная модель ПВКК

Результатом функционирования предлагаемой ПВКК является выработанный ею КК, предназначенный для введения в загрузчик ключей СКЗИ в составе системы ЗИ КФС. База лиц F представляет собой множество разрешенных образов – наборов БмД определенных субъектов, при этом для F предусмотрена возможность оперативного изменения ее содержания.

На рис. 2 представлен результат декомпозиции блока A0 контекстной диаграммы, приведенной на рис. 1. Предлагаемая схема позволяет получить более полное представление о принципах функционирования ПВКК.

Гипотеза: ПВКК со способностями, соответствующими функциональному наполнению блоков A1, A2, A3, A4, реализуема.

Для проверки гипотезы предлагается перейти от формализма функционального моделирования к формализмам теории алгоритмов, имеющим достаточную историю применения [30] при исследованиях проблем информационной безопасности. С учетом функциональной эквивалентности аппаратного и программного обеспечения абстрагируемся от его конкретного воплощения и будем на основании тезиса Тьюринга считать вычислительную систему реализуемой при существовании моделирующего ее работу алгоритма, формализованного любым из принятых в теории алгоритмов способов. Алгоритм предназначен для разрешения массовой или алгоритмической проблемы, формализуемой

своим языком L_{MP} – множеством слов, описывающими проблему [9, 14]. Используем следующие обозначения, принятые в теории алгоритмов: $A(x,y)=z$ – алгоритм A останавливается на входе x,y с результатом z; запись $A_\alpha \circ A_\beta = A_\gamma$ обозначает, что A_γ является результатом последовательной композиции алгоритмов A_α и A_β. Далее в целях сокращения объема статьи примем, что все входы и выходы алгоритмов представляют собой слова, кодирующие определенные ранее соответствующие объекты, т.е. вместо традиционной записи $code(L)$ будем писать L, подразумевая $code(L)$, и т.д. Принятые обозначения позволяют сформулировать алгоритмическую проблему P_{KK}, отражающую задачу рассмотренной выше модели, формализуемую языком

$$L_{KK}=\left\{\left(f_i,L,R,P\right)_g,k_i\right\},\ g=\overline{1,N_G}, \tag{1}$$

где k_i – КК с номером i, $i=\overline{1,N_I}$.

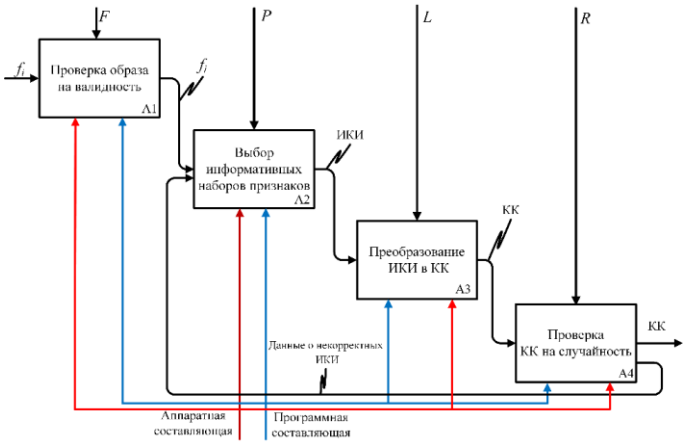

Рис. 2. Второй уровень функциональной модели ПВКК

Разрешимость L_{KK} будет означать, что существует алгоритм $A^0\left(f_i,L,R,P\right)_g=k_i$, ставящий в однозначное соответствие каждому входу $\left(f_i,L,R,P\right)_g$ конкретный КК k_i. Следует отметить, что набор (L,R,P), являющийся элементом управления модели на рис. 1 и 2, помещен в часть языка (1), подаваемую на вход A^0, по причине перехода от абстракций функционального моделирования к теоретико-алгоритмическим, предполагающим, что управляющие инструкции могут содержаться только в самом алгоритме или в его входе. С целью проверки выдвинутой гипотезы сформулирована следующая **теорема**: массовая проблема выработки КК, формализуемая языком L_{KK}, разрешима алгоритмом с нетривиальными семантическими свойствами, соответствующими функциональному наполнению блоков A1, A2, A3, A4.

Доказательство теоремы. Рассмотрим предлагаемое алгоритмическое содержание представленных блоков второго уровня функциональной модели, что обеспечит переход от использования методологии IDEF0 к теоретико-алгоритмическому описанию моделируемых процессов. Указанный переход, обоснованный в [14], согласуется с положениями системного подхода к построению и исследованию моделей. Для осуществления перехода поставим в соответствие каждому блоку Ai модели, приведенной на рис. 2, реализующий его функционал алгоритм A^i, т.е. зададим отображение $\text{A}i \xrightarrow{M} A^i$.

В блоке А1 осуществляется проверка поступившего на вход ПВКК образа f_i на принадлежность F, т.е. реализуется разрешающий конечное множество F алгоритм

$$A^1(f_i)=\begin{cases} f_i, \text{ если } f_i \in F; \\ 0 \text{ иначе,} \end{cases}$$

являющийся по сути алгоритмом, разрешающим известную массовую проблему сравнения двух слов в конечном их множестве.

При получении $A^1(f_i)=0$ функционирование ПВКК останавливается по недопуску слова, соответствующего набору БмД f_i.

Следует отметить, что в рассматриваемой модели не отражен важный [31] вопрос качества получаемого на вход блока А1 образа f_i, при решении которого применительно к рассматриваемому классу КФС необходимо учитывать ограниченность ресурсов.

В блоке А2 из поступившего на вход набора f_i осуществляется выбор информативных признаков на основе P, т.е. вычисление слова p_i алгоритмом вида

$$A^2(f_i,P)=p_i\ .$$

Указанное действие необходимо для выбора из f_i набора уникальных признаков, способных обеспечить выработку на их основе множества КК, удовлетворяющих заданным требованиям безопасности. Таким образом, на выход блока А2 поступает информативный набор БмД в виде слова p_i, полученный путем обработки f_i, и представляющий собой исходную ключевую информацию (ИКИ), под которой понимается совокупность данных, предназначенных для выработки из них по определенным правилам КК [16].

Блок А3 иллюстрирует этап выработки КК требуемой длины L из ИКИ p_i, поступившей из Блока А2, т.е. вычисление

$$A^3(p_i,L)=k_i,$$

где $k_i \in \{1,0\}^+$, $|k_i|=L$.

Блок А4 иллюстрирует необходимый этап проверки выработанного КК на случайность с учетом множества доступных для ПВКК алгоритмов тестирования $T=\{\Theta_p\}$, $p=\overline{1,N_P}$, системы C правил определения количества N_r и выбора тестов из T, определяющих своей совокупностью $R=\langle N_r,T,C\rangle$. Система тестирования будет реализовываться последовательным выполнением в отношении k_i, вычисленного A^3, r алгоритмов тестирования, рассмотренных подробно в [32],

$$\Theta_r(k_i)=\begin{cases} 1, \text{ если } k_i \text{ прошел } r\text{-й тест;} \\ 0 \text{ иначе.} \end{cases}$$

Проверка КК на случайность, являющаяся наполнением А4, будет реализовываться следующим алгоритмом:

$$A^4(k_i,\Theta_r)=\begin{cases} k_i, \text{ если } \bigcap_{r_j}^{|\Theta_r|}\Theta_r(k_i)=1; \\ 0 \text{ иначе.} \end{cases}$$

Рассмотренные алгоритмы позволяют сделать вывод о том, что моделирующий функционирование ПВКК алгоритм $A(f_i,L,R,P)=k_i$ может быть представлен как композиция уже рассмотренных

$$A^0=A^1\circ A^2\circ A^3\circ A^4,$$

что, в свою очередь, позволяет делать вывод о разрешимости P_{KK} с языком (1). □

Выводы. Изложенные в работе предложения могут рассматриваться в качестве одного из направлений исследований по унификации СКЗИ РТК и являющихся их обобщением – КФС. Однако для этого, кроме исследований в области технологий, необходимо изменение существующей системы взглядов регуляторов на выработку КК, разработку СКЗИ и обращение с ними. Продолжение исследования видится в решении актуальной проблемы выбора оптимального набора средств защиты информации [11], учитывающего рассмотренные выше особенности применения РТК и вопросы информационной безопасности их ресурсов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Wang X., Guo Y., Gao Y.* Unmanned Autonomous Intelligent System in 6G Non-Terrestrial Network // Information. – 2024. – Vol. 15, No. 1:38. – URL: https://doi.org/10.3390/info15010038.
2. Science & Technology Trends 2023-2043. Overview. NATO Science & Technology Organization. – URL: https://cesmar.it/wp-content/uploads/2023/04/stt23-vol1.pdf.
3. *Honey D.A.* Trusted AI and autonomy for today's warfighter // Autonomous Systems: Sensors, Processing, and Security for Ground, Air, Sea, and Space Vehicles and Infrastructure 2024. – SPIE, 2024. – Vol. 13052. – P. 130520E.
4. *Chafii M., Bariah L., Muhaidat S., Debbah M.* Twelve Scientific Challenges for 6G: Rethinking the Foundations of Communications Theory // IEEE Communications Surveys & Tutorials. – 2023. – Vol. 25, Issue 2. – P. 868-904.
5. *Blakcori N., Stathakis L.I., Koutsoukos L.D., Kirilov L.K.* The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements // NATO, Integrated Air and Missile Defence Center of Excellence. – 2024. – 18 p.
6. *Турдаков Д.Ю., Аветисян А.И., Архипенко К.В., Анциферова А.В., Ватолин Д.С., Волков С.С., Гасников А.В. и др.* Доверенный Искусственный интеллект: вызовы и перспективные решения // Доклады Российской академии наук. Математика, информатика, процессы управления. – 2022. – Т. 508, №1. – С. 13-18.
7. *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.
8. *Головенкин А.С.* Проблема ограниченности ресурсов в обеспечении экономической безопасности предприятий оборонно-промышленного комплекса // Вестник евразийской науки. – 2024. – Т. 16, № S1.
9. *Головской В.А.* Операционная модель когнитивной радиосистемы робототехнического комплекса // T-Comm: Телекоммуникации и транспорт. – 2024. – Т. 18, № 5. – С. 12-20.
10. *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.
11. *Головской В.А.* Алгоритмические аспекты проблемы оценивания достаточности средств защиты информации // Перспективы безопасности-2024: Сб. материалов II научно-технической конференции, посвященной информационной безопасности, Санкт-Петербург, 19–20 июня 2024 года. – СПб.: ООО «Специальный Технологический Центр», 2024. – С. 17-22.
12. *Бочаров Н.А.* Исследование подходов к унификации бортовых вычислительных комплексов // Известия ЮФУ. Технические науки. – 2023. – № 1 (231). – С. 275-287.
13. *Gnutov M.S., Sizonenko A.B., Gnutov S.K.* Optimization of Resource Utilization of Distributed Automated Systems Under the Influence of Heterogeneous Security Threats // Proceedings of the 2nd 2020 International Youth Conference on Radio Electronics, Electrical and Power Engineering, REEPE 2020, Moscow, 12–14.03.2020. – Moscow: Institute of Electrical and Electronics Engineers Inc., 2020. – P. 9059180.
14. *Головской В.А.* Анализ проблематики прогнозирования поведения когнитивных радиосистем // Радиотехника. – 2024. – Т. 88, № 12. – С. 134-145.
15. *Молдовян Н.А., Горячев А.А., Муравьев А.В.* Протокол стойкого шифрования по ключу малого размера // Вопросы защиты информации. – 2015. – № 1 (108). – С. 3-8.
16. 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. – 87 с.

17. *Микони С.В.* Методика построения многоуровневой модели оценивания сложного объекта // Онтология проектирования. – 2022. – Т. 12, № 3 (45). – С. 380-392.
18. *Pham H.L., Trung Duong Le V., Duy Tran V., Hai Vu T., Nakashima Y.* LiCryptor: High-Speed and Compact Multi-Grained Reconfigurable Accelerator for Lightweight Cryptography // IEEE Transactions on Circuits and Systems I: Regular Papers. – 2024. – Vol. 71, No. 10. – P. 4624-4637.
19. *Поляков А.В.* Биометрическое личностное шифрование // Интеллектуальные системы. Теория и приложения. – 2017. – Т. 21, № 1. – С. 149-163.
20. *Бабенко Л.К., Русаловский И.Д.* Разработка операций для алгоритмов гомоморфного шифрования // Вопросы кибербезопасности. – 2024. – № 2 (60). – С. 101-106.
21. *Duong Le V.T., Pham H.L., Duong T.S., Tran T.H., Nam Nguyen Q.D., Nakashima Y.* RHCP: A Reconfigurable High-efficient Cryptographic Processor for Decentralized IoT Platforms // 2023 15th International Conference on Knowledge and Systems Engineering (KSE), Hanoi, Vietnam, 2023. – P. 1-6.
22. *Shamir A.* Identity-Based Cryptosystems and Signature Schemes // Advances in Cryptology. – 1985. – Vol. 196. – P. 47-53.
23. *Куликов А.А.* Применение биометрических систем в технологиях идентификации лиц // Российский технологический журнал. – 2021. – № 9 (3). – С. 7-14.
24. *Mizinov P.V., Konnova N.S., Basarab M.A., Pleshakova E.S.* Parametric study of hand dorsal vein biometric recognition vulnerability to spoofing attacks // Journal of Computer Virology and Hacking Techniques. – 2023. – Vol. 20. – P. 383-396.
25. *Баянов Б.И.* Метод квантования с линейным преобразованием биометрических данных динамического рукописного почерка // Вестник технологического университета. – 2023. – Т. 26, № 1. – С. 113-118.
26. *Волчихин В.И., Иванов А.И., Иванов А.П.* Алгоритм быстрого вычисления энтропии Шеннона на малых выборках для длинных кодов биометрии с существенно зависимыми разрядами // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2024. – № 4. – С. 27-34.
27. *Сулавко А.Е., Ложников П.С., Самотуга А.Е., Сулавко А.В., Стадников Д.Г., Чобан А.Г.* Идентификационный потенциал электроэнцефалограмм в задачах информационной безопасности: монография. – Омск: Изд-во ОмГТУ, 2025. – 264 с.
28. *Рыбалов А.Н.* О генерической сложности проблемы дискретного логарифма в последовательностях Люка // Прикладная дискретная математика. – 2024. – № 66. – С. 116-122.
29. *Куракин А.С.* Модель разграничения прав доступа виртуального отряда беспилотных летательных аппаратов // Проблемы информационной безопасности. Компьютерные системы. – 2022. – № 3. – С. 121-129.
30. *Cohen F.* Computational aspects of computer viruses // Computers & Security. – 1989. – Vol. 8, No. 4. – P. 297-298.
31. *Schlett T., Rathgeb C, Henniger O., Galbally J., Fierrez J., Busch C.* Face Image Quality Assessment: A Literature Survey // ACM Computing Surveys (CSUR). – 2022. – Vol. 54, Issue 10s. – P. 1-49.
32. *Иванов А.И.* Нейросетевой многокритериальный статистический анализ малых выборок. Проверка гипотезы независимости. – Пенза: Изд-во ПГУ, 2023. – 218 с.

REFERENCES

1. *Wang X., Guo Y., Gao Y.* Unmanned Autonomous Intelligent System in 6G Non-Terrestrial Network, *Information*, 2024, Vol. 15, No. 1:38. Available at: https://doi.org/10.3390/info15010038.
2. Science & Technology Trends 2023-2043. Overview. NATO Science & Technology Organization. Available at: https://cesmar.it/wp-content/uploads/2023/04/stt23-vol1.pdf.
3. *Honey D.A.* Trusted AI and autonomy for today's warfighter, *Autonomous Systems: Sensors, Processing, and Security for Ground, Air, Sea, and Space Vehicles and Infrastructure 2024*. SPIE, 2024, Vol. 13052, pp. 130520E.
4. *Chafii M., Bariah L., Muhaidat S., Debbah M.* Twelve Scientific Challenges for 6G: Rethinking the Foundations of Communications Theory, *IEEE Communications Surveys & Tutorials*, 2023, Vol. 25, Issue 2, pp. 868-904.
5. *Blakcori N., Stathakis L.I., Koutsoukos L.D., Kirilov L.K.* The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements, *NATO, Integrated Air and Missile Defence Center of Excellence*, 2024, 18 p.
6. *Turdakov D.Yu., Avetisyan A.I., Arkhipenko K.V., Antsiferova A.V., Vatolin D.S., Volkov S.S., Gasnikov A.V. i dr.* Doverennyy Iskusstvennyy intellekt: vyzovy i perspektivnye resheniya [Trusted artificial intelligence: challenges and promising solutions], *Doklady Rossiyskoy akademii nauk. Matematika, informatika, protsessy upravleniya* [Reports of the Russian Academy of Sciences. Mathematics, informatics, control processes], 2022, Vol. 508, No. 1, pp. 13-18.

7. *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, pp. 399-408.
8. *Golovenkin A.S.* Problema ogranichennosti resursov v obespechenii ekonomicheskoy bezopasnosti predpriyatiy oboronno-promyshlennogo kompleksa [The problem of limited resources in ensuring the economic security of enterprises of the military-industrial complex], *Vestnik evraziyskoy nauki* [The Eurasian Scientific Journal], 2024, Vol. 16, № S1.
9. *Golovskoy V.A.* Operatsionnaya model' kognitivnoy radiosistemy robototekhnicheskogo kompleksa [An operational model of the cognitive radio system of a robotic complex], *T-Comm: Telekommunikatsii i transport* [T-Comm: Telecommunications and transport], 2024, Vol. 18, No. 5, pp. 12-20.
10. *Biryukov P.A., Timokhin A.A., Makarenko S.I.* Brigady sukhoputnykh voysk, vooruzhennye bespilotnymi letatel'nymi apparatami: obosnovanie sozdaniya, predlozheniya po ikh strukture, sposobam boevogo primeneniya i tekhnicheskomu obespecheniyu s uchetom opyta spetsial'noy voennoy operatsii na Ukraine [Brigades of ground forces equipped with unmanned aerial vehicles: justification for their creation, proposals on their structure, methods of combat use and technical support, taking into account the experience of the special military operation in Ukraine], *Sistemy upravleniya, svyazi i bezopasnosti* [Systems of Control, Communication and Security], 2024, No. 2, pp. 43-70.
11. *Golovskoy V.A.* Algoritmicheskie aspekty problemy otsenivaniya dostatochnosti sredstv zashchity informatsii [Algorithmic aspects of the problem of assessing the adequacy of information security tools], *Perspektivy bezopasnosti-2024: Sb. materialov II nauchno-tekhnicheskoy konferentsii, posvyashchennoy informatsionnoy bezopasnosti, Sankt-Peterburg, 19–20 iyunya 2024 goda* [Security Prospects-2024: Proceedings of the II Scientific and Technical Conference on Information Security, St. Petersburg, June 19-20, 2024]. Saint Petersburg: OOO «Spetsial'nyy Tekhnologicheskiy Tsentr», 2024, pp. 17-22.
12. *Bocharov N.A.* Issledovanie podkhodov k unifikatsii bortovykh vychislitel'nykh kompleksov [Study of approaches to the unification of on-board computers], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2023, No. 1 (231), pp. 275-287.
13. *Gnutov M.S., Sizonenko A.B., Gnutov S.K.* Optimization of Resource Utilization of Distributed Automated Systems Under the Influence of Heterogeneous Security Threats, *Proceedings of the 2nd 2020 International Youth Conference on Radio Electronics, Electrical and Power Engineering, REEPE 2020, Moscow, 12–14.03.2020*. Moscow: Institute of Electrical and Electronics Engineers Inc., 2020, pp. 9059180.
14. *Golovskoy V.A.* Analiz problematiki prognozirovaniya povedeniya kognitivnykh radiosistem [Analysis of the problems of predicting the behavior of cognitive radio systems], *Radiotekhnika* [Radioengineering], 2024, Vol. 88, No. 12, pp. 134-145.
15. *Moldovyan N.A., Goryachev A.A., Murav'ev A.V.* Protokol stoykogo shifrovaniya po klyuchu malogo razmera [Protocol for secure encryption with using small-size key], *Voprosy zashchity informatsii* [Information security questions], 2015, No. 1 (108), pp. 3-8.
16. MR 26.2.006-2021. Metodicheskie rekomendatsii «Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Terminy i opredeleniya». Tekhnicheskiy komitet po standartizatsii TK 26 «Kriptograficheskaya zashchita informatsii» [MP 26.2.006-2021. Methodological recommendations «Information technology. Cryptographic protection of information. Terms and definitions». Technical Committee for Standardization «Cryptographic information Protection»]. Moscow, 2021, 87 p.
17. *Mikoni S.V.* Metodika postroeniya mnogourovnevoy modeli otsenivaniya slozhnogo ob"ekta [Methodology for creating a multilevel model for evaluating a complex object], *Ontologiya proektirovaniya* [Ontology of designing], 2022, Vol. 12, No. 3 (45), pp. 380-392.
18. *Pham H.L., Trung Duong Le V., Duy Tran V., Hai Vu T., Nakashima Y.* LiCryptor: High-Speed and Compact Multi-Grained Reconfigurable Accelerator for Lightweight Cryptography, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2024, Vol. 71, No. 10, pp. 4624-4637.
19. *Polyakov A.V.* Biometricheskoe lichnostnoe shifrovanie [Biometric identity encryption], *Intellektual'nye sistemy. Teoriya i prilozheniya* [Intelligent systems. Theory and applications], 2017, Vol. 21, No. 1, pp.149-163.
20. *Babenko L.K., Rusalovskiy I.D.* Razrabotka operatsiy dlya algoritmov gomomorfnogo shifrovaniya [Development of operations for homomorphic encryption algorithms], *Voprosy kiberbezopasnosti* [Voprosy kiberbezopasnosti], 2024, No. 2 (60), pp. 101-106.
21. *Duong Le V.T., Pham H.L., Duong T.S., Tran T.H., Nam Nguyen Q.D., Nakashima Y.* RHCP: A Reconfigurable High-efficient Cryptographic Processor for Decentralized IoT Platforms, *2023 15th International Conference on Knowledge and Systems Engineering (KSE), Hanoi, Vietnam, 2023*, pp. 1-6.
22. *Shamir A.* Identity-Based Cryptosystems and Signature Schemes, *Advances in Cryptology*, 1985, Vol. 196, pp. 47-53.

23. *Kulikov A.A.* Primenenie biometricheskikh sistem v tekhnologiyakh identifikatsii lits [Application of biometric systems in face identification technologies], *Rossiyskiy tekhnologicheskiy zhurnal* [Russian Technological Journal], 2021, No. 9 (3), pp. 7-14.
24. *Mizinov P.V., Konnova N.S., Basarab M.A., Pleshakova E.S.* Parametric study of hand dorsal vein biometric recognition vulnerability to spoofing attacks, *Journal of Computer Virology and Hacking Techniques*, 2023, Vol. 20, pp. 383-396.
25. *Bayanov B.I.* Metod kvantovaniya s lineynym preobrazovaniem biometricheskikh dannykh dinamicheskogo rukopisnogo pocherka [Quantization method with linear transformation of biometric data of dynamic handwriting], *Vestnik tekhnologicheskogo universiteta* [Herald of Technological University], 2023, Vol. 26, No. 1, pp. 113-118.
26. *Volchikhin V.I., Ivanov A.I., Ivanov A.P.* Algoritm bystrogo vychisleniya entropii Shennona na malykh vyborkakh dlya dlinnykh kodov biometrii s sushchestvenno zavisimymi razryadami [Algorithm for fast computation of Shannon's entropy on small samples for long biometrics codes with essentially dependent digits], Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: *Upravlenie, vychislitel'naya tekhnika i informatika* [Vestnik of Astrakhan state technical university. Series: Management, computer science and informatics], 2024, No. 4, pp. 27-34.
27. *Sulavko A.E., Lozhnikov P.S., Samotuga A.E., Sulavko A.V., Stadnikov D.G., Choban A.G.* Identifikatsionnyy potentsial elektroentsefalogramm v zadachakh informatsionnoy bezopasnosti: monografiya [The identification potential of electroencephalograms in information security tasks]. Omsk: Izd-vo OmGTU, 2025, 264 p.
28. *Rybalov A.N.* O genericheskoy slozhnosti problemy diskretnogo logarifma v posledovatel'nostyakh Lyuka [On the generic complexity of the discrete logarithm problem in Lucas sequences], *Prikladnaya diskretnaya matematika* [Applied discrete mathematics], 2024, No. 66, pp. 116-122.
29. *Kurakin A.S.* Model' razgranicheniya prav dostupa virtual'nogo otryada bespilotnykh letatel'nykh apparatov [A model of differentiation of access rights for a virtual squad of unmanned aerial vehicles], *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Problems of information security. Computer systems], 2022, No. 3, pp. 121-129.
30. *Cohen F.* Computational aspects of computer viruses, *Computers & Security*, 1989, Vol. 8, No. 4, pp. 297-298.
31. *Schlett T., Rathgeb C, Henniger O., Galbally J., Fierrez J., Busch C.* Face Image Quality Assessment: A Literature Survey, *ACM Computing Surveys (CSUR)*, 2022, Vol. 54, Issue 10s, pp. 1-49.
32. *Ivanov A.I.* Neyrosetevoy mnogokriterial'nyy statisticheskiy analiz malykh vyborok. Proverka gipotezy nezavisimosti [Neural network multicriterial statistical analysis of small samples. Testing the hypothesis of independence]. Penza: Izd-vo PGU, 2023, 218 p.

Головской Василий Андреевич – Краснодарское высшее военное училище им. генерала армии С.М. Штеменко; e-mail: golovskoy_va@mail.ru; 350063, г. Краснодар, Россия; тел.: +79384762531; к.т.н.; доцент; начальник кафедры.

Винокуров Александр Владимирович – Краснодарское высшее военное училище им. генерала армии С.М. Штеменко; e-mail: vav73@rambler.ru; 350063, г. Краснодар, Россия; тел.: +79604913609; д.т.н.; доцент; профессор кафедры.

Golovskoy Vasiliy Andreevich – Krasnodar Higher Military School named after S.M. Shtemenko; e-mail: golovskoy_va@mail.ru; Krasnodar, Russia; phone: +79384762531; cand. of eng. sc.; assistant of professor; head of the chair.

Vinokurov Alexander Vladimirovich – Krasnodar Higher Military School named after S.M. Shtemenko; e-mail: vav73@rambler.ru; Krasnodar, Russia; phone: +79604913609; cand. of eng. sc.; associate professor; professor.