Автоматизация и моделирование в проектировании и управлении. 2025. № 4 (30). С. 58-64.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2025. № 4 (30). P. 58-64.

Научная статья
Статья в открытом доступе
УДК 004.056
doi: 10.30987/2658-6436-2025-4-58-64

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОНТРОЛЯ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАТЕГИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Наталия Михайловна Кузнецова[1], Татьяна Владимировна Карлова[2]
[1] Московский государственный технологический университет «СТАНКИН», г. Москва, Россия
[2] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[1] knm87@mail.ru
[2] karlova-t@yandex.ru

Аннотация. *Целью является повышение уровня информационной безопасности стратегически важных объектов железнодорожного транспорта и их вспомогательных информационных и автоматизированных систем, за счет проектирования модели автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов. Для достижения поставленной цели сформулированы основные задачи автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта, представлены архитектура проектируемой автоматизированной системы, методика оптимизации архитектуры. Новизной работы является предложенная креативная концепция оптимизации архитектуры проектируемой автоматизированной системы за счет применения основных положений ГОСТ Р 70569–2022 «Информационные технологии. Сетецентрические инфромационно-управляющие системы. Интероперабельность», что позволит минимизировать время принятия управленческого решения, повысить надежность передачи конфиденциальных данных. Результатом исследования являются рекомендации по проектированию автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта, а также методика оптимизации ее архитектуры.*

Ключевые слова: автоматизация, защита информации, информационная безопасность, защита от целевых атак, защита от физических угроз, предотвращение реализации физических угроз

Для цитирования: Кузнецова Н.М., Карлова Т.В. Проектирование автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта // Автоматизация и моделирование в проектировании и управлении. 2025. №4 (30). С. 58-64. doi: 10.30987/2658-6436-2025-4-58-64.

Original article
Open Access Article

DESIGNING AN AUTOMATED SYSTEM FOR MONITORING INFORMATION SECURITY PARAMETERS OF CRITICAL RAILWAY TRANSPORTATION FACILITIES

Natalya M. Kuznetsova[1], Tatyana V. Karlova[2]
[1] Moscow State University of Technology «STANKIN», Moscow, Russia
[2] Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[1] knm87@mail.ru
[2] karlova-t@yandex.ru

Abstract. *The aim of this study is to enhance the level of information security for critical railway transportation facilities and their auxiliary information and automated systems through designing an automated system model for controlling information security parameters of critical facilities. To achieve this aim the authors formulate the main tasks of the automated system for monitoring information security parameters of critical railway transport facilities, and present the architecture of the designed automated system, as well as the methodology for optimizing the architecture. The novelty of the work lies in the proposed creative concept of optimizing the architecture of the designed automated*

system by applying the main provisions of GOST R 70569–2022 "Information Technologies. Network-centric Information-control Systems. Interoperability," which will minimize the time required for decision-making and increase the reliability of confidential data transmission. The outcome of the study includes recommendations for designing an automated system for monitoring information security parameters of critical railway transportation facilities, as well as a methodology for optimizing its architecture.

Keywords: automation, information protection, information security, defence against targeted attacks, defence against physical threats, prevention of physical threat realization

For citation: Kuznetsova N.M., Karlova T.V. Designing an Automated System for Monitoring Information Security Parameters of Critical Railway Transportation Facilities. Automation and modeling in design and management, 2025, no. 4 (30). pp. 58-64. doi: 10.30987/2658-6436-2025-4-58-64.

Введение

Актуальной задачей является повышение уровня информационной безопасности стратегически важных объектов железнодорожного транспорта (мостов, тоннелей, железнодорожных перегонов и т.д.). Данные объекты являются стратегически важными, ввиду их роли в поддержании общей транспортной инфраструктуры страны. Кроме того, в условиях цифровизации [1], данные объекты, как правило, оснащены соответствующими вспомогательными информационными и автоматизированными системами (ВИиАС). В свою очередь, для ВИиАС стратегически важных объектов железнодорожного транспорта также необходимо обеспечение должного уровня безопасности данных [2 – 7]. Статья посвящена решению поставленных задач защиты данных за счет внедрения автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта (АСКПИБ).

Основные задачи автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта

К основным задачам АСКПИБ относятся:

– постоянный контроль уровня информационной безопасности стратегически важных объектов железнодорожного транспорта и ВИиАС за счет отслеживания значений параметров;

– своевременное детектирование снижения уровня информационной безопасности стратегически важных объектов железнодорожного транспорта и ВИиАС;

– своевременное реагирование:

а) оповещение о снижении уровня информационной безопасности стратегически важных объектов железнодорожного транспорта и ВИиАС;

б) предотвращение снижения уровня информационной безопасности стратегически важных объектов железнодорожного транспорта и ВИиАС.

Проектирование архитектуры автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта

Как правило, стратегически важные объекты железнодорожного транспорта и составные части ВИиАС территориально распределены. В связи с этим, АСКПИБ должна иметь клиент-серверную архитектуру.

На рис. 1 представлена архитектура АСКПИБ.

Основными достоинствами представленной архитектуры АСКПИД являются:

– возможность масштабирования за счет увеличения объектов на стороне клиента;

– высокая степень гибкости за счет принципа модульного построения;

– высокая степень управляемости за счет серверной стороны (центрального управления).

При этом, сохраняется принцип «вертикали власти»: иерархичности узлов управления. Однако главным недостатком иерархического построения АСКПИД является увеличение времени принятия управленческого решения в случае, когда данное решение касается «соседних» стратегически важных объектов железнодорожного транспорта и соответствующих ВИиАС.

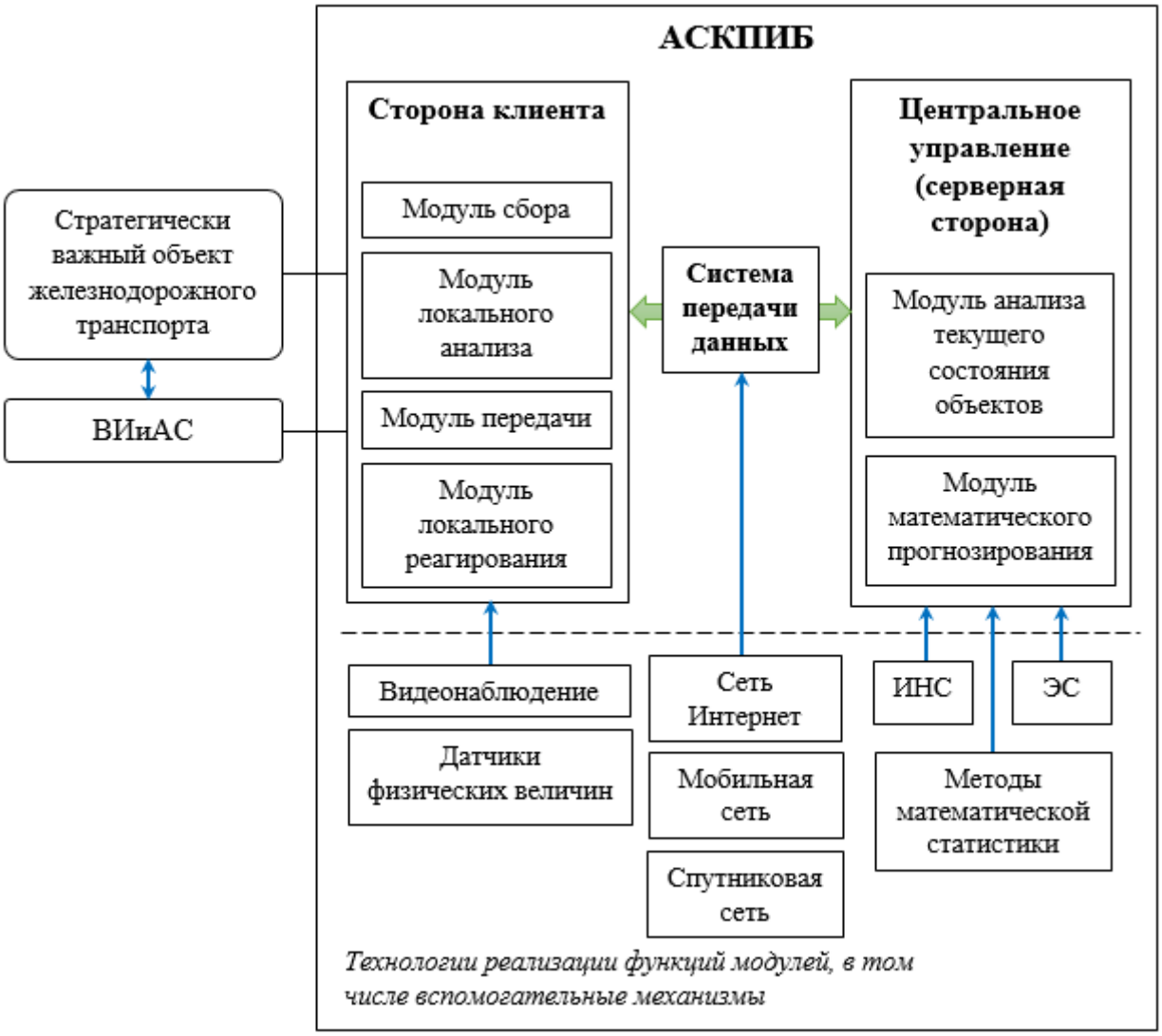

Рис. 1. Архитектура АСКПИД
Fig. 1. Architecture of ASKPID

Сторона клиента автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта. Согласно рис. 1, стратегически важные объекты железнодорожного транспорта и ВИиАС связаны напрямую именно с клиентской стороной АСКПИД.

Клиентскую сторону АСКПИД составляют модули: модуль сбора; модуль локального анализа; модуль передачи; модуль локального реагирования.

Модуль сбора обеспечивает фиксацию данных, полученных от датчиков стратегически важных объектов железнодорожного транспорта, а также значений параметров соответствующих ВИиАС для проведения дальнейшего анализа.

Модуль локального анализа необходим для того, чтобы реагировать на инциденты информационной безопасности незамедлительно «на месте» (на соответствующей стороне клиента АСКПИД).

Модуль передачи обеспечивает транспортировку данных от клиентской стороны на серверную с помощью системы передачи данных.

Модуль локального реагирования необходим для своевременного предотвращения реализаций угроз информационной безопасности посредством методов оповещения, блокировки доступа, нейтрализации угрозы, а также карантинных мер информационной безопасности [8].

Серверная сторона (центральное управление) автоматизированной системы контроля

параметров информационной безопасности стратегически важных объектов железнодорожного транспорта. Серверную сторону АСКПИД составляют модули: модуль анализа текущего состояния объектов; модуль математического прогнозирования.

Модуль анализа текущего состояния стратегически важных объектов железнодорожного транспорта и соответствующих ВИиАС производит общее «глобальное» исследование всех данных, полученных от всех клиентских сторон АСКПИД. Подобный анализ позволяет оценить общую «картину» уровня информационной безопасности всех стратегически важных объектов железнодорожного транспорта, что в свою очередь позволяет своевременно детектировать попытки реализации комплексных целевых кибератак (*APT – Advanced Persistent Threats*), которые на данный момент считаются наиболее опасными [9 – 12].

Модуль математического прогнозирования:

– анализирует всю поступившую информацию о текущем состоянии параметров информационной безопасности стратегически важных объектов железнодорожного транспорта, а также ВИиАС;

– прослеживает динамику изменений значений данных параметров;

– производит анализ рисков изменения общего уровня информационной безопасности.

Система передачи данных. Главными задачами системы передачи данных АСКПИД являются: сохранение целостности передаваемых данных; обеспечение конфиденциальности передаваемых данных.

Задача сохранения целостности решается за счет механизмов дублирования каналов связи.

Задача обеспечения конфиденциальности передаваемых данных решается за счет применения криптографических методов [13 – 15].

Технологии реализации функций модулей автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта. К технологиям реализации функций модулей и вспомогательным механизмам АСКПИД относятся:

– механизмы видеонаблюдения (для модуля сбора клиентской стороны);

– датчики физических величин (для модуля сбора клиентской стороны);

– сеть Интернет (для системы передачи данных);

– мобильная сеть (для системы передачи данных);

– спутниковая сеть (для системы передачи данных);

– искусственные нейронные сети (ИНС) (для модуля анализа текущего состояния объектов, модуля математического прогнозирования серверной стороны);

– экспертные системы (ЭС) (для модуля анализа текущего состояния объектов, модуля математического прогнозирования серверной стороны);

– методы математической статистики, в том числе методы Монте-Карло (для модуля математического прогнозирования серверной стороны) [16].

В табл. 1 представлено соответствие использования вспомогательных механизмов модулями АСКПИД.

Таблица 1
Table 1

Соответствие использования вспомогательных механизмов модулями АСКПИД
Correspondence of the use of auxiliary mechanisms by the ASKPID modules

Технология реализации и вспомогательные механизмы	Модуль	Часть АСКПИД
Механизмы видеонаблюдения	Модуль сбора	Клиентская сторона
Датчики физических величин		
Сеть Интернет	Система передачи данных	
Мобильная сеть		
Спутниковая сеть		
ИНС	Модуль анализа текущего состояния объектов, модуль математического прогнозирования	Серверная сторона
ЭС		
Методы математической статистики	Модуль математического прогнозирования	

Схема передачи информации для принятия решения в иерархической архитектуре АСКПИД представлена на рис. 2. Схема передачи информации для принятия решения в сетевой архитектуре АСКПИД представлена на рис. 3.

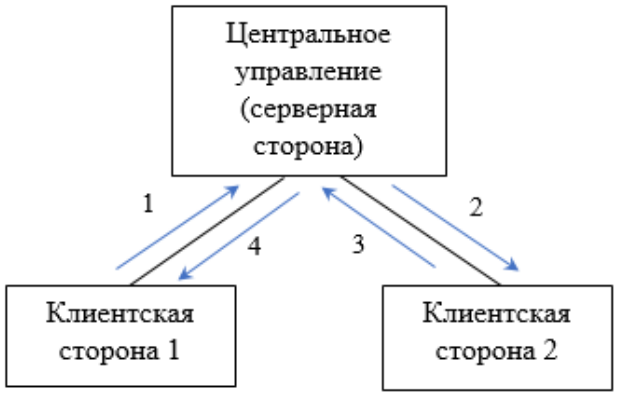

Рис. 2. Схема передачи информации для принятия решения в иерархической архитектуре АСКПИД
Fig. 2. Information transfer diagram for decision-making in the hierarchical ASKID architecture

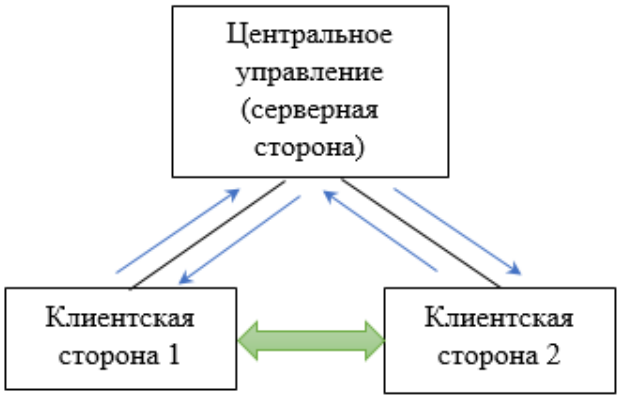

Рис. 3. Схема передачи информации для принятия решения в сетевой архитектуре АСКПИД
Fig. 3. Information transfer scheme for decision-making in the ASKPID network architecture

Согласно рис. 2, передача данных от одной клиентской стороны АСКПИД к другой в иерархической архитектуре производится в четыре этапа: через серверную сторону АСКПИД (при этом, помимо передачи данных, от серверной части поступают управляющие сигналы). В то время как при сетевой архитектуре АСКПИД, построенной по сетецентрическому принципу согласно положениям ГОСТ Р 70569–2022 [17], клиентские части обмениваются данными напрямую, что минимизирует время принятия решения:

$$t(\sum_{i=1}^{N} p_i) \rightarrow \min \quad (1)$$

где N – общее число анализируемых параметров информационной безопасности стратегически важных объектов железнодорожного транспорта и соответствующих ВИиАС, p – значение анализируемого параметра.

Если в иерархической архитектуре от центрального управления передавались как данные, так и управляющие сигналы, то в сетевой архитектуре от одной клиентской стороны к другой передаются только данные (сигналы оповещения).

При этом важно отметить, что связь с серверной стороной сохраняется, что в свою очередь повышает надежность передачи данных. Кроме того, данные передаются на серверную сторону для общей статистики.

Представленная методика сетевой архитектуры АСКПИД удовлетворяет требованиям ГОСТ Р 70569–2022 [17].

Заключение

Приведенная в статье модель проектирования автоматизированной системы контроля параметров информационной безопасности стратегически важных объектов железнодорожного транспорта позволит своевременно детектировать и реагировать на инциденты информационной безопасности, предотвратить реализацию угроз информационной безопасности, в том числе комплексных целевых атак, что в свою очередь значительно повысит уровень защиты стратегически важных объектов железнодорожного транспорта и их вспомогательных информационных и автоматизированных систем.

Список источников:

1. Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р Об утверждении стратегического направления в области цифровой трансформации государственного управления.

2. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Построение модульной структуры автоматизированной системы комплексного обеспечения защиты стратегически важных ресурсов предприятия транспорта // Вестник Брянского государственного технического университета. – 2021. – № 9 (106). – С. 36-42.

3. Кузнецова Н.М. Применение биометрической аутентификации в автоматизированных системах защиты стратегически важных ресурсов предприятия (монография). – М.: «Янус-К», 2023. – 136 с.

4. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Проектирование вспомогательной автоматизированной системы принятия управленческих решений на основе анализа уровня информационной безопасности // Автоматизация и моделирование в проектировании и управлении. – 2023. – № 3 (21). – С. 13-22.

5. Кузнецова Н.М., Карлова Т.В. Применение технологии цифровых двойников для моделирования уровня информационной безопасности промышленного предприятия // Моделирование нелинейных процессов и систем. Материалы пятой международной конференции (Москва, 16–20 ноября 2020 г.). – М.: Янус–К, 2021. – С. 224-225.

6. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Применение методов математического моделирования для оценки эффективности автоматизированных систем защиты интеллектуальных ресурсов промышленных предприятий // Моделирование нелинейных процессов и систем. Материалы шестой международной конференции. – М: Янус-К, 2023. – с. 163-166.

7. Formation of an Intellectual Resource of an Enterprise Using Virtual and Augmented Reality Technologies Based on Sociodynamics Methods / Kuznetsova N.M., Karlova T.V. et al. // Proceedings of the 2024 International Conference «Quality Management, Transport and Information Security, Information Technologies», QM and TIS and IT 2024. – 2024. – с. 159-161.

8. Кузнецова Н.М. Методология защиты от целевых кибератак повышенной сложности в автоматизированных системах промышленного предприятия (монография). – М.: «Янус-К», 2024. – 132с.

9. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибер-атак на основе анализа тактик злоумышленников // Вестник Брянского государственного технического университета. – № 7(92). – 2020. – С. 48-53.

10. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Y. Method of Timely Prevention from Advanced Persistent Threats on the Enterprise Automated Systems // 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)

References:

1. On Approval of the Strategic Direction in the Field of Digital Transformation of Public Administration. Decree of the Government of the Russian Federation No. 2998-r; 2021 Oct 22.

2. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Construction of a Modular Structure of an Automated System for Integrating Support for the Protection of Strategically Important Resources of a Transport Enterprise. Bulletin of Bryansk State Technical University. 2021;9(106):36-42.

3. Kuznetsova N.M. Application of Biometric Authentication in Automated System of Critical Enterprise Resource Protection. Moscow: Janus-K; 2023.

4. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Designing an Auxiliary Automated Management Decision-Making System Based on Information Security Level Analysis. Automation and Modelling in Design and Management. 2023;3(21):13-22.

5. Kuznetsova NM, Karlova TV. Application of Digital Twin Technology for Modelling of Information Security Level of Industrial Enterprise. In: Proceedings of the 5th International Conference on Modelling of Non-Linear Processes and Systems; 2020 Nov 16-20; Moscow: Janus-K: 2021. p. 224-225.

6. Kuznetsova NM, Karlova TV, Bekmeshov AY. Application of Mathematical Modelling Methods for Evaluating the Efficiency of Automated Systems for the Protection of Intellectual Resources of Industrial Enterprises. In: Proceedings of the 6th International Conference on Modelling of Non-Linear Processes and Systems. Moscow: Janus-K: 2023. p. 163-166.

7. Kuznetsova NM, Karlova TV, et al. Formation of an Intellectual Resource of an Enterprise Using Virtual and Augmented Reality Technologies Based on Sociodynamics Methods. In: Proceedings of the 2024 International Conference on Quality Management, Transport and Information Security, Information Technologies (QM and TIS and IT); 2024. p. 159-161.

8. Kuznetsova N.M. Methodology of Protection Against Targeted Cyber Attacks of Increased Complexity in Automated Systems of an Industrial Enterprise. Moscow: Yanus-K; 2024.

9. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Solution of Protection Automation Problem of Company Strategic Resources Against Complex Cyberattacks Based on Criminal Tactics Analysis. Bulletin of Bryansk State Technical University. 2020;7(92):48-53.

10. Kuznetsova NM, Karlova TV, Bekmeshov AY. Method of Timely Prevention from Advanced Persistent Threats on the Enterprise Automated Systems. In: Proceedings of the 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS); 2022. p. 158-161.

11. Кузнецова Н.М., Карлова Т.В. Основные принципы защиты автоматизированных систем крупных промышленных предприятий от комплексных кибер-атак // Вестник Брянского государственного технического университета. – 2017. – № 4 (57). – С. 84-89.

12. Methods Dedicated to Fight Against Complex Information Security Theats on Automated Factories Systems / T.V. Karlova, N.M. Kuznetsova et al. // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS) // Proceedings. – М.: Фонд «Качество». – 2016. – P. 23-27.

13. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студ. высш. учеб. заведений – 4-е изд., стер. – М.: Издательский центр «Академия», 2008 – 256 с.

14. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях // М.: Горячая линия – Телеком, 2021. – 432 с.

15. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.

16. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Автоматизированное моделирование распространения инфекционных заболеваний среди населения мегаполиса с помощью метода Монте Карло с учётом аспектов информационной безопасности // Качество. Инновации. Образование. – 2020. – № 5 (169). – С. 96-102.

17. ГОСТ Р 70569–2022 «Информационные технологии. Сетецентрические инфромационно-управляющие системы. Интероперабельность»: ФГБУ «Институт стандартизации», 2022.

11. Kuznetsova N.M., Karlova T.V. Basic Principles for Large Enterprise Automated System Protection Against Cyber Attacks. Bulletin of Bryansk State Technical University. 2017;4(57):84-89.

12. Karlova TV, Kuznetsovaet NM, et al. Methods Dedicated to Fight Against Complex Information Security Threats on Automated Factories Systems. In: Proceedings of the 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS); 2016 Oct 04-16; Nalchik (RF). New-York: IEEE: 2016. p. 72-76, doi: 10.1109/ITMQIS.2016.7751927

13. Khorev P.B. Methods and Means of Information Protection in Computer Systems. 4th ed. Moscow: Akademiya; 2008.

14. Miloslavskaya N.G. Scientific Foundations for Building Network Security Management Centres in Information and Tele-Communication Networks. Moscow: Hot Line-Telecom; 2021.

15. Panasenko S.P. Encryption Algorithms: Special Reference Book. Saint Petersburg: BHV-Peterburg; 2009.

16. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Y. Automated Monte Carlo Simulation of Epidemic Spread in Megacity Population Accounting for Information Security Aspects. Quality. Innovations. Education. 2020;5(169):96-102.

17. GOST R 70569-2022. Information Technologies. Network-Centric Information-Control Systems. Interoperability. Moscow: Standardization Institute; 2022.

Информация об авторах:

Кузнецова Наталия Михайловна
кандидат технических наук, доцент Московского государственного технологического университета «СТАНКИН».

Карлова Татьяна Владимировна
доктор социологических наук, кандидат технических наук, профессор Института конструкторско-технологической информатики Российской академии наук.

Information about the authors:

Kuznetsova Natalya Mikhailovna
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology «STANKIN»

Karlova Tatyana Vladimirovna
Doctor of Sociology, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 20.10.2025; одобрена после рецензирования 18.11.2025; принята к публикации 28.11.2025.

The article was submitted 20.10.2025; approved after reviewing 18.11.2025; accepted for publication 28.11.2025.

Рецензент – Малаханова А.Г., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Malakhanova A.G., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.