**DOI: 10.12731/2227-930X-2024-14-4-308** **EDN: XIFNRS**
**УДК 004.056**



Научная статья | Управление процессами перевозок

# КИБЕРБЕЗОПАСНОСТЬ В СФЕРЕ ТРАНСПОРТА

***О.В. Князькина, Р.М. Хамитов, О.П. Черникова, Ю.А. Златицкая***

***Аннотация***

Стремительные темпы научно-технического прогресса в отношении информатизации и цифровизации общества влекут за собой риск возрастания киберугроз, которые представляют серьезную проблему для организаций, поскольку темпы развития цифровых и информационных технологий существенно опережают темпы развития инструментов для их защиты. В статье описывается актуальность вопросов кибербезопасности в сфере транспорта, приводится понятийный аппарат кибербезопасности и основные типы кибератак. Изучена статистика киберугроз на транспорте в 2023 году по сравнению с 2022 годом. Рассмотрена киберсреда и основные элементы ее защиты. Разработана процедура управления кибербезопасностью в транспортной организации, в основе которой заложен процессный подход к управлению кибербезопасностью, включающая в себя блок по управлению аудитом текущего состояния системы защиты в организации и блок с последовательностью действий в случае наступления кибератаки. Предложенная процедура управления кибербезопасностью позволяет не только предотвращать потенциальные кибератаки, но производить аудит текущего состояния киберзащиты и формировать направления по ее совершенствованию с учетом изменяющихся угроз и динамично развивающихся технологий.

**Цель** – изучение вопросов управления кибербезопасностью в транспортной организации в условиях возрастания рисков киберугроз.

**Метод и методология проведения работы.** В статье использовались методы теории систем, системного анализа и синтеза, аналитические и статистические методы.

**Результаты.** Изучена статистика киберугроз в сфере транспорта. Предложена процедура управления кибербезопасностью в транспортной организации, позволяющая управлять оценкой текущего состояния системы защиты в организации и регламентирующая порядок действий в случае наступления кибератаки.

**Область применения результатов.** Полученные результаты исследования могут быть востребованы в практике управления вопросами кибербезопасности в транспортной организации.

**Ключевые слова:** сфера транспорта; кибербезопасность; кибератака; цифровизация; информатизация процессов; киберсреда

**Для цитирования.** Князькина О.В., Хамитов Р.М., Черникова О.П., Златицкая Ю.А. Кибербезопасность в сфере транспорта // International Journal of Advanced Studies. 2024. Т. 14, № 4. С. 29-45. DOI: 10.12731/2227-930X-2024-14-4-308

Original article | Transportation Process Management

## CYBER SECURITY IN TRANSPORTATION

***O.V. Knyazkina, R.M. Khamitov,***
***O.P. Chernikova, Yu.A. Zlatitskaya***

***Abstract***

The fast pace of scientific and technological progress in terms of informatisation and digitalisation of society entails the risk of increasing cyber threats, which pose a serious problem for organisations, as the pace of development of digital and information technologies significantly outstrips the pace of development of tools to protect them. The article describes the relevance of cyber security issues in the transport sector, provides a conceptual framework of cyber security and the main types of cyber attacks. The statistics of cyber threats in transport in 2023 compared to 2022 is studied. The cyber environment and the main elements of its defence are considered. A procedure for managing cyber security in a transport organisation has been developed, which is based on a process approach to

cyber security management, including a block for managing the audit of the current state of the defence system in the organisation and a block with a sequence of actions in the event of a cyber attack. The proposed cyber security management procedure allows not only to prevent potential cyber attacks, but also to audit the current state of cyber defence and form directions for its improvement, taking into account changing threats and dynamically developing technologies.

**Purpose.** To study the issues of cybersecurity management in a transport organization in conditions of increasing risks of cyber threats.

**Methodology.** The article uses methods of systems theory, system analysis and synthesis, analytical and statistical methods.

**Results.** The statistics of cyber threats in the transport sector is studied. A procedure for managing cyber security in a transport organisation is proposed, which makes it possible to manage the assessment of the current state of the organisation's protection system and regulates the procedure for actions in the event of a cyber attack.

**Practical implications.** The obtained research results may be in demand in the practice of cyber security management in a transport organisation.

**Keywords:** transport; cyber security; cyberattack; digitalization; informatization of processes; cyber environment

**For citation.** Knyazkina O.V., Khamitov R.M., Chernikova O.P., Zlatitskaya Yu.A. Cyber Security in Transportation. *International Journal of Advanced Studies,* 2024, vol. 14, no. 4, pp. 29-45. DOI: 10.12731/2227-930X-2024-14-4-308

**Введение**

Транспорт представляет собой жизненно важную отрасль экономики, в которой задействованы различные организации: компании, работающие в сфере логистики, предприятия городского транспорта, перевозчики, нацеленные как на перевозку пассажиров, так и грузов силами автомобильного, воздушного, водного, авиационного, железнодорожного транспорта и прочие. За прошедшее десятилетие сфера транспорта претерпела существенные

изменения, активно идет информатизация и цифровизация транспортных процессов, отмечается быстрое развитие программных продуктов и техники, применяются инструменты искусственного интеллекта и комплексы для автоматизированного управления технологическими и техническими процессами. Внедрение информационных технологий в сфере транспорта в первую очередь ориентировано на повышение эффективности процессов за счет повышения результативности организации и управления транспортных и логистических процессов, повышения рентабельности перевозок, роста фондовооруженности труда, снижения себестоимости транспортных услуг, повышение уровня безопасности и т.д. По мере того как транспортная отрасль становится все более цифровой возрастает риск киберугроз [2; 11-15].

Сфера транспорта выполняет важные функции в масштабах государства, поскольку выступает в качестве связующего звена как между регионами страны, так и между всеми сферами экономики, следовательно, предприятия транспортной отрасли являются объектом повышенного внимания и могут быть подвержены кибератакам, то есть вопрос актуальности кибербезопасности в сфере транспорта не вызывает сомнений.

**Понятийный аппарат**

Кибербезопасность – свойства различных программно-управляемых систем автоматического управления сохранять способность к безопасному и эффективному выполнению возложенных на них функциональных задач в условиях целенаправленных, умышленных, несанкционированно-деструктивных воздействий различной физической природы [7].

В сложившейся ситуации перед предприятиями транспортной сферы возникает задача по формированию мероприятий, направленных на достижение и непрерывное совершенствование кибербезопасности, нацеленной на обеспечение способности информационно-цифровой системы предприятия к функционированию

в условиях кибератак различной природы. Основные типы кибератак приведены на рисунке 1 [3; 6; 7].

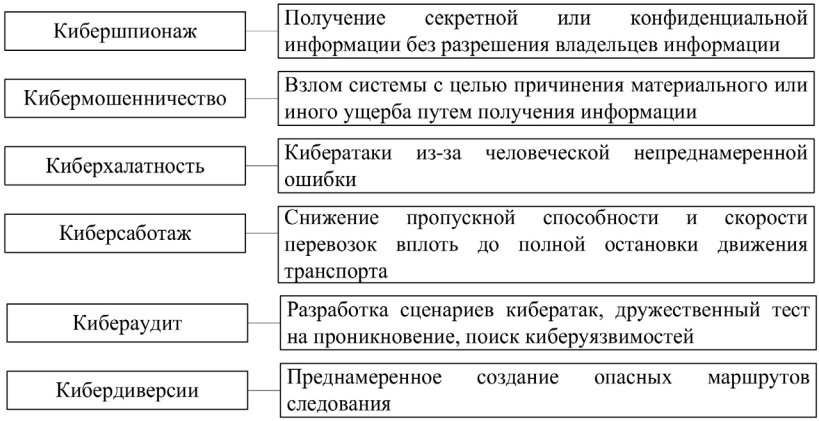


**Рис. 1.** Основные типы кибератак

**Статистика кибератак в сфере транспорта**

По данным Positive Technologies [5], в 2023 г. по сравнению с 2022 г. количество успешных кибератак в сфере транспорта в мировом масштабе увеличилось на 36% что обусловлено общим ростом числа кибератак. Наиболее популярным направлениями кибератак в 2023 г. (около 87%) являются компьютеры, серверы и сетевое оборудование, порядка 50% кибератак направлено на веб-ресурсы компаний, 20% атак нацелено на людей в основном путем рассылки фишинговых писем и лишь 4% кибератак направлено на прочие объекты (рис.2).

Кибератаки в сфере транспорта могут привести к сбоям в бизнес-процессах и задержкам в оказании транспортных услуг. Так в результате кибератак может быть нарушена работа системы онлайн-бронирования, от кибератак могут пострадать внутренние операции транспортной организации, что приведет к задержкам в доставке грузов и увеличению эксплуатационных расходов. Также, воздействию кибератак могут быть подвержены системы обеспечения безопасности пассажиров, что создаст угрозу для клиентов и работников сферы

транспорта. Иногда кибератаки нацелены на вымогательство денег у организации путем угрозы проведения кибератаки.

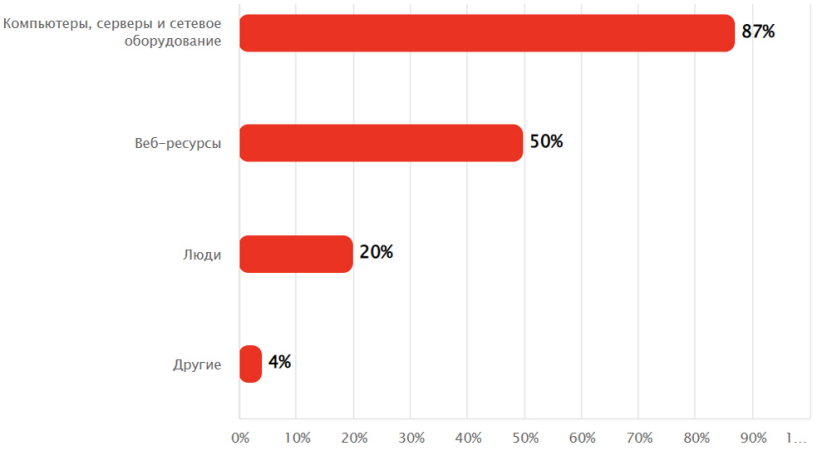


**Рис. 2.** Структура кибератак [5]

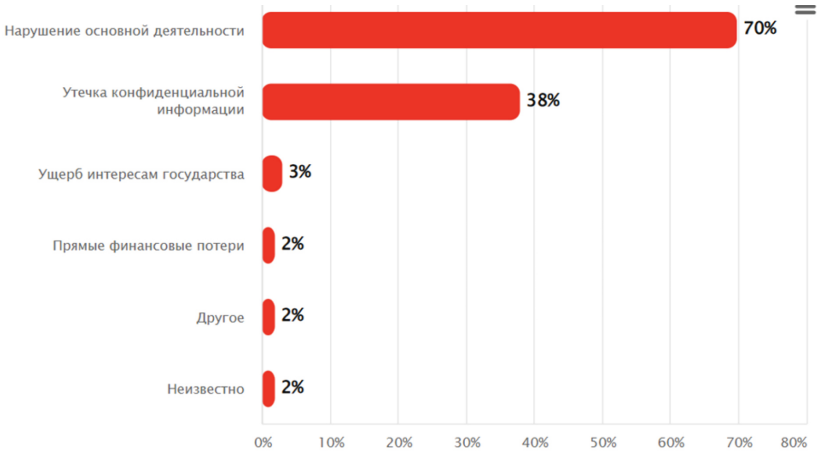


**Рис. 3.** Последствия кибератак для организаций в сфере транспорта [5]

В 2023 г. примерно в 70% транспортных компаний в следствие кибератак отмечалось нарушение основной деятельности:

наблюдались сбои в предоставлении сервисов клиентам, потеря доступа к инфраструктуре или данным внутри организаций, нарушение внутренних бизнес-процессов. У 38% организаций наблюдалась утечка конфиденциальной информации, а в результате 3% кибератак был нанесен ущерб интересам государства (рис. 3).

**Постановка задачи**

Кибербезопасность представляет серьезную проблему для организаций в сфере транспорта, поскольку темпы развития цифровых и информационных технологий существенно опережают темпы развития инструментов для их защиты. Если рассматривать транспортную сферу с позиции системного подхода, то транспортные организации по сути, представляют собой открытые системы, оказывающие транспортные услуги. Поскольку транспортные организации функционируют в условиях конкуренции, то особое значение приобретают показатели рентабельности, прибыльности транспортного предприятия и привлекательности для клиентов, на что оказывают непосредственное влияние скорость перевозки, логистика и параметры формирования маршрутов доставки, оптимизация использования транспортных средств, активность внедрения цифровых и информационных технологий. В этой связи возникает задача управления обеспечением защитой киберсреды транспортной организации, от угроз, связанных с цифровыми технологиями.

**Киберсреда и основные элементы ее защиты**

Киберсреда транспортных организаций представляет собой систему информационно-коммуникационных технологий и цифровых ресурсов организации, которая возникает в результате взаимодействия потребителей транспортных услуг (грузоотправителей, грузополучателей и пассажиров), персонала транспортных организаций, программного обеспечения, комплексов автоматизированного управления, цифровой среды, инструментов искусственного интеллекта и интернет-технологий. Основные элемен-

ты защиты киберсреды транспортной организации приведены на рисунке 4 [1; 9].


**Рис. 4.** Основные элементы защиты киберсреды транспортной организации

Учитывая, что в будущем кибератаки станут одним из основных бизнес-рисков в транспортной сфере, то к управлению кибербезопасностью целесообразно подходить с позиции процессного подхода с акцентом на превентивную направленность. Рассмотрим процедуру управления кибербезопасностью транспортной организации, в основе которой лежит работа в двух направлениях: порядок действия в случае возникновения кибератак и непрерывное совершенствование действующей киберзащиты (рис. 5).

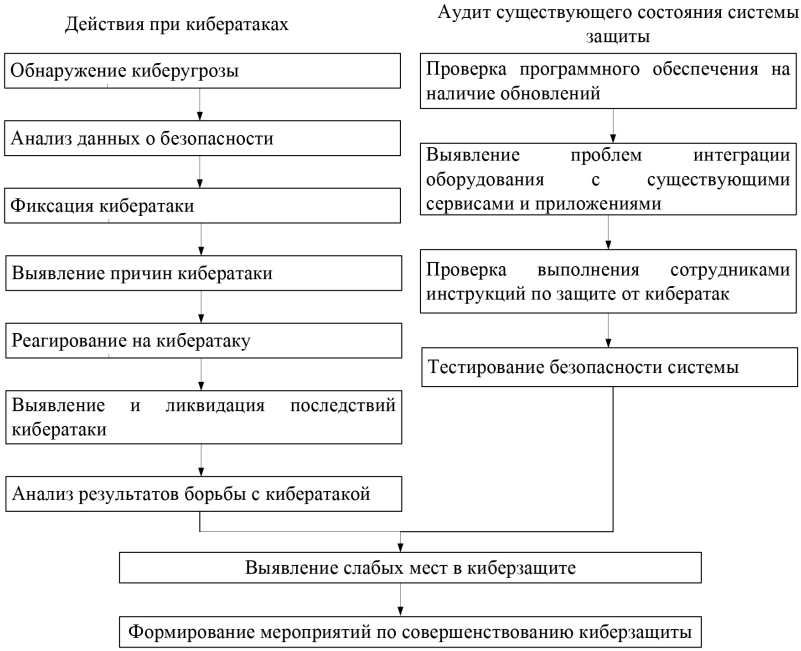


**Рис. 5.** Процедура управления кибербезопасностью в транспортной организации

## Заключение

Вопрос кибербезопасности в транспортной отрасли представляет собой актуальную и значимую проблему, требующую серьезного внимания и системного подхода. Развитие процессов цифровизации и информатизации в данной отрасли сопровожда-

ется увеличением киберугроз, что может привести к серьезным последствиям, таким как нарушение бизнес-процессов, утечка конфиденциальной информации и угрозы для безопасности пассажиров. Изучение статистики кибератак в сфере транспорта позволяет определить основные направления угроз и их потенциальные последствия для организаций.

Особое внимание следует уделить разработке процедур управления кибербезопасностью, которые помогут не только предотвращать атаки, но и проводить аудит текущего состояния киберзащиты и формировать направления для ее совершенствования. Ключевую роль в обеспечении безопасности информационных систем транспортной организации играют элементы защиты киберсреды, такие как сегментация сети, программное обеспечение для защиты конечных узлов, регулярные исправления и обновления программного обеспечения, резервное копирование данных, обучение по вопросам кибербезопасности, глубокая защита и тестирование безопасности.

Процессный подход к управлению кибербезопасностью в транспортной отрасли предполагает не только реагирование на потенциальные кибератаки, но и активное усовершенствование системы защиты с учетом изменяющихся угроз и технологий. Важными компонентами такого подхода являются обучение сотрудников, регулярное тестирование безопасности и постоянное обновление систем защиты. Таким образом, внедрение эффективных мер по обеспечению кибербезопасности в транспортной отрасли является необходимым шагом к минимизации рисков и обеспечению бесперебойного функционирования транспортных организаций.

Различные отрасли народного хозяйства страны, такие как металлургия и машиностроение, аграрная промышленность и животноводство, водо- и энергоснабжение, телекоммуникации и прочие для обеспечения своего функционирования напрямую зависят от транспортной сферы. Значительный сбой в транспортной отрасли, предположительно, может привести к беспрецедентно-

му ущербу. В этой связи предложенная процедура управления кибербезопасностью в транспортной организации, в основе которой заложен процессный подход к управлению кибербезопасностью, позволяет не только предотвращать кибератаки, но производить аудит текущего состояния киберзащиты и формировать направления по совершенствованию киберзащиты.

### *Список литературы*

1. Аввакумова А.А. Обеспечение информационной безопасности на транспорте / А.А. Аввакумова, А.А. Трефилова // Аспект. URL: https://na-journal.ru/8-2023-informacionnye-tekhnologii/6196-obespechenie-informacionnoi-bezopasnosti-na-transporte (дата обращения: 22.04.2024).
2. Васильев Е. А. Кибербезопасность в интеллектуальных транспортных системах / Е. А. Васильев, О. В. Князькина // Поколение будущего: Взгляд молодых ученых–2023: сборник научных статей 12-й Международной молодежной научной конференции, 9–10 ноября 2023 г.: в 4-х т. / отв. ред. Горохов А. А. Курск, 2023. Т. 3. С. 45–48.
3. Журавлева Н.А. Проблемы экономической безопасности транспортных систем в условиях глобальных киберугроз / Н.А. Журавлева, А.Б. Никитин // Экономические науки. 2018. № 11 (168). С. 20-25.
4. Исмагилов И. Р. Моделирование угроз безопасности при защите объектов критически важной информационной инфраструктуры / И. Р. Исмагилов, Р. И. Ахметшина, Э. А. Гильманова // Экономика и социум. 2022. № 2-2(93). С. 645-648.
5. Киберугрозы в транспортной отрасли // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/ (дата обращения: 22.04.2024).
6. Киселева Е.М. Железная дорога как объект // Международный студенческий научный вестник. 2018. № 5. URL: https://eduherald.ru/ru/article/view?id=19179 (дата обращения: 22.04.2024).

7. Макаров Б.А. Актуальность кибербезопасности на железнодорожном транспорте // Техника железных дорог. 2015. №3 (31). С. 19-24
8. Натальсон А. В. Оценка риска нарушения информационной безопасности в банковской сфере // Современные цифровые технологии: проблемы, решения, перспективы : национальная (с международным участием) научно-практическая конференция, Казань, 19–20 мая 2022 года. Казань: Казанский государственный энергетический университет, 2022. С. 113-116.
9. Основные проблемы кибербезопасности в транспортном секторе // tmc3: сайт. URL: https://www.tmc3.co.uk/insights/cyber-security-challenges-in-the-transport-sector (дата обращения 22.04.2024).
10. Хамитов Р. М. Использование искусственного интеллекта в безопасности на транспорте / Р. М. Хамитов, О. В. Князькина // Наука и молодежь: проблемы, поиски, решения: труды Всероссийской научной конференции студентов, аспирантов и молодых ученых, Новокузнецк, 16–17 мая 2023 года. Новокузнецк: Сибирский государственный индустриальный университет, 2023. С. 3-6.
11. Al Ali, N. A. R. Cyber security in marine transport: Opportunities and legal challenges / N. A. R. Al Ali, A. A. Chebotareva, V. E. Chebotarev // Pomorstvo. 2021. Vol. 35, No. 2. P. 248-255. https://doi.org/10.31217/p.35.2.7
12. Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity / V. Lakhno, B. Akhmetov, A. Korchenko [et al.] // Journal of Theoretical and Applied Information Technology. 2018. Vol. 96, No. 14. P. 4530-4540.
13. Ishmuratov R.A., Kalabanov S.A., Shagiev R.I., Onischuk M.V. Monitoring and Control System of Three-Phase Electrical Loads on Railway Trains // 2020 IEEE East-West Design and Test Symposium, EWDTS 2020 - Proceedings 9225142.
14. Kolchurina I., Kolchurina M., Khamitov R., Plotnikova I. Usage Practice of Information Technology for the Reorganization of Production Processes // Lysenko E., Rogachev A., Galtseva O. (eds) Emerging Trends in Materials Research and Manufacturing Processes. Engineering Materials. Springer, Cham. 2023. https://doi.org/10.1007/978-3-031-38964-1_8

15. Kutsenko S. M. Diagnostics of high-voltage insulation of the railway transport overhead system by the method of spaced antennas / S. M. Kutsenko, N. N. Klimov // IOP Conference Series: Materials Science and Engineering: International Conference on Transport and Infrastructure of the Siberian Region, SibTrans 2019, Moscow, May 21-24, 2019. Vol. 760. Moscow: Institute of Physics Publishing, 2020. P. 012035. https://doi.org/10.1088/1757-899X/760/1/012035
16. Mentsiev A. Digital transformation in transport infrastructure energy efficiency: Smart cities and sustainable mobility / A. Mentsiev, U. Takhaev, A. Mentsiev // E3S Web of Conferences, St. Petersburg, September 19-21, 2023. Vol. 460. St. Petersburg: EDP Sciences, 2023. P. 07018. https://doi.org/10.1051/e3sconf/202346007018

## *References*

1. Avvakumova A.A. Ensuring information security in transportation / A.A. Avvakumova, A.A. Trefilova. *Aspect*. URL: https://na-journal.ru/8-2023-informacionnye-tekhnologii/6196-obespechenie-informacionnoi-bezopasnosti-na-transporte
2. Vasiliev E. A. Cybersecurity in intelligent transportation systems / E. A. Vasiliev, O. V. Knyazkina. *Generation of the Future: The View of Young Scientists-2023: collection of scientific articles of the 12th International Youth Scientific Conference, November 9-10, 2023*: in 4 vol. / edited by A. A. Gorokhov. Kursk, 2023. Vol. 3. P. 45-48.
3. Zhuravleva N.A. Problems of economic security of transportation systems in the context of global cyber threats / N.A. Zhuravleva, A.B. Nikitin. *Economic Sciences,* 2018, no. 11 (168), pp. 20-25.
4. Ismagilov I. R. Modeling of security threats in the protection of critical information infrastructure objects / I. R. Ismagilov, R. I. Akhmetshina, E. A. Gilmanova. *Economics and Socium,* 2022, no. 2-2(93), pp. 645-648.
5. Cyber threats in the transportation industry. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/

6. Kiseleva E.M. Railroad as an object. *International Student Scientific Bulletin,* 2018, no. 5. URL: https://eduherald.ru/ru/article/view?id=19179
7. Makarov B.A. Actuality of cybersecurity on the railway transportation. *Technics of railroads,* 2015, no. 3 (31), pp. 19-24
8. Natalson A. V. Risk assessment of information security violation in the banking sector. *Modern digital technologies: problems, solutions, prospects: national (with international participation) scientific-practical conference, Kazan, May 19-20, 2022*. Kazan: Kazan State Power Engineering University, 2022, pp. 113-116.
9. Main problems of cyber security in the transportation sector. *tmc3: website*. URL: https://www.tmc3.co.uk/insights/cyber-security-challenges-in-the-transport-sector
10. Khamitov R. M. The use of artificial intelligence in transportation security / R. M. Khamitov, O. V. Knyazkina. *Science and youth: problems, searches, solutions: proceedings of the All-Russian scientific conference of students, graduate students and young scientists, Novokuznetsk, May 16-17, 2023*. Novokuznetsk: Siberian State Industrial University, 2023, pp. 3-6.
11. Al Ali, N. A. R. Cyber security in marine transportation: Opportunities and legal challenges / N. A. R. Al Ali, A. A. Chebotareva, V. E. Chebotarev. *Pomorstvo,* 2021, vol. 35, no. 2, pp. 248-255. https://doi.org/10.31217/p.35.2.7
12. Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity / V. V. Lakhno, B. A. A. Chebotarev. Lakhno, B. Akhmetov, A. Korchenko [et al.]. *Journal of Theoretical and Applied Information Technology,* 2018, vol. 96, no. 14, pp. 4530-4540.
13. Ishmuratov R.A., Kalabanov S.A., Shagiev R.I., Onischuk M.V. Monitoring and Control System of Three-Phase Electrical Loads on Railway Trains. *2020 IEEE East-West Design and Test Symposium, EWDTS 2020 - Proceedings* 9225142.
14. Kolchurina I., Kolchurina M., Khamitov R., Plotnikova I. Usage Practice of Information Technology for the Reorganization of Production

Processes / Lysenko E., Rogachev A., Galtseva O. (eds). *Emerging Trends in Materials Research and Manufacturing Processes. Engineering Materials*. Springer, Cham. 2023. https://doi.org/10.1007/978-3-031-38964-1_8

15. Kutsenko S. M. Diagnostics of high-voltage insulation of the railway transport overhead system by the method of spaced antennas / S. M. Kutsenko. M. Kutsenko, N. N. Klimov. *IOP Conference Series: Materials Science and Engineering: International Conference on Transport and Infrastructure of the Siberian Region, SibTrans 2019, Moscow, May 21-24, 2019*. Vol. 760. Moscow: Institute of Physics Publishing, 2020, p. 012035. https://doi.org/10.1088/1757-899X/760/1/012035
16. Mentsiev A. Digital transformation in transport infrastructure energy efficiency: Smart cities and sustainable mobility / A. Mentsiev, U. Mentsiev. Mentsiev, U. Takhaev, A. Mentsiev. *E3S Web of Conferences, St. Petersburg, September 19-21, 2023*. Vol. 460. St. Petersburg: EDP Sciences, 2023, p. 07018. https://doi.org/10.1051/e3sconf/202346007018

## ДАННЫЕ ОБ АВТОРАХ

**Князькина Ольга Владимировна,** доцент кафедры «Транспорта и логистики», кандидат технических наук
*Сибирский государственный индустриальный университет*
*ул. Кирова, 42, г. Новокузнецк, Кемеровская область - Кузбасс, 654007, Российская Федерация*
*dmtov@mail.ru*

**Хамитов Ренат Минзашарифович,** доцент кафедры «Информационные технологии и интеллектуальные системы», кандидат технических наук
*Казанский государственный энергетический университет*
*ул. Красносельская, 51, г. Казань, Республика Татарстан, 420066, Российская Федерация*
*hamitov@gmail.com*

**Черникова Оксана Петровна,** заведующий кафедрой «Экономики, учета и финансов», кандидат экономических наук
*Сибирский государственный индустриальный университет*
*ул. Кирова, 42, г. Новокузнецк, Кемеровская область - Кузбасс, 654007, Российская Федерация*
*chernikovaop@yandex.ru*

**Златицкая Юлия Александровна**, доцент кафедры «Экономики, учета и финансов», кандидат технических наук
*Сибирский государственный индустриальный университет*
*ул. Кирова, 42, г. Новокузнецк, Кемеровская область - Кузбасс, 654007, Российская Федерация*
*zlatitskaya@bk.ru*

## DATA ABOUT THE AUTHORS

**Olga V. Knyazkina,** Associate Professor «Transport and Logistics», Candidate of Technical Sciences
*Siberian State Industrial University*
*42, Kirova Str., Novokuznetsk, Kemerovo region - Kuzbass, 654007, Russian Federation*
*dmtov@mail.ru*
*SPIN-code: 2657-2162*
*ORCID: https://orcid.org/0000-0002-1448-3061*

**Renat M. Khamitov,** Associate Professor «Information Technologies and Intelligent Systems», Candidate of Technical Sciences
*Kazan State Power Engineering University*
*51, Krasnoselskaya Str., Kazan, Tatarstan, 420066, Russian Federation*
*hamitov@gmail.com*
*SPIN-code: 7401-9166*
*ORCID: https://orcid.org/0000-0002-9949-4404*

**Oksana P. Chernikova,** Head of the Department of «Economics, Accounting and Finance», Candidate of Economic Sciences
*Siberian State Industrial University*
*42, Kirova Str., Novokuznetsk, Kemerovo region - Kuzbass, 654007, Russian Federation*
*chernikovaop@yandex.ru*
*SPIN-code: 6496-5060*
*ORCID: https://orcid.org/0000-0002-5410-6623*

**Yulia A. Zlatitskaya,** Associate Professor of the Department of "Economics, Accounting and Finance", Candidate of Technical Sciences
*Siberian State Industrial University*
*42, Kirova Str., Novokuznetsk, Kemerovo region - Kuzbass, 654007, Russian Federation*
*zlatitskaya@bk.ru*
*SPIN-code: 9135-6180*
*ORCID: https://orcid.org/0009-0009-0393-0514*

Поступила 20.10.2024 Received 20.10.2024
После рецензирования 01.11.2024 Revised 01.11.2024
Принята 05.11.2024 Accepted 05.11.2024