DOI: 10.12731/3033-5965-2025-15-4-385 **EDN: GRQUDG**
УДК 656.61:351.86:007

Научная статья | Транспортные и транспортно-технологические системы

СОСТОЯНИЕ СИНГУЛЯРНОСТИ БЕЗОПАСНОСТИ: ПЕРЕХОД К РЕФЛЕКСИВНОЙ СИСТЕМЕ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

А.Е. Ранверсман

Аннотация

Обоснование. В исследовании обосновывается необходимость введения понятийного и модельного инструментария, позволяющего отразить динамику эволюции системы обеспечения транспортной безопасности. Развитие транспортного комплекса сопровождается изменениями, которые затрагивают инфраструктуру, технические средства и распределение функций между человеком и технологическим контуром, что приводит к формированию новых принципов управления безопасностью. В этой связи возникает потребность в аналитической модели уровней зрелости (C0-C5), которая позволяет проследить направление эволюции и определить структурные признаки перехода от регламентированных процедур к рефлексивному управлению. Одновременно вводится понятие «состояние сингулярности безопасности» как предельное состояние зрелости системы обеспечения транспортной безопасности, достигаемое за счёт перехода к саморегуляции и объединения технических, аналитических и человеческих компонентов в единый рефлексивный контур.

Цель – теоретическое обоснование концепции состояния сингулярности безопасности и разработка модели уровней зрелости (C0-C5) системы обеспечения транспортной безопасности, отражающей переход от традиционных организационно-регламенти-

рованных процедур к интеллектуально-адаптивным механизмам упреждения угроз.

Материалы и методы. Главный метод исследования – моделирование, использованное для разработки модели уровней зрелости и построения рефлексивного контура функционирования системы обеспечения транспортной безопасности. Методологическую основу составляет системный и междисциплинарный подход, опирающийся на теории управления сложными и социотехническими системами, кибернетический подход и риск-ориентированную логику. Теоретическую и нормативную базу составили правовые акты Российской Федерации, международные документы ICAO и EASA, а также стратегические материалы Минтранса и Международного транспортного форума. В исследовании применялись системно-структурный и нормативно-правовой анализ, контент-анализ стратегических документов и логико-прогностические методы.

Результаты. В ходе исследования разработана модель уровней зрелости (C0-C5) и введено понятие «состояние сингулярности безопасности» как предельное состояние зрелости системы обеспечения транспортной безопасности. Оно характеризует этап, при котором система достигает уровня саморефлексии и саморегуляции, где механизмы реагирования и предотвращения угроз основаны на непрерывной самообновляемой модели управления рисками, а технические средства, аналитические модули и человеческое участие объединяются в единый рефлексивный контур. Полученные результаты могут быть использованы для диагностики уровня зрелости системы, определения направления её дальнейшей эволюции и обоснования требований к подготовке специалистов в условиях цифровой трансформации.

Ключевые слова: транспортная безопасность; модель уровней зрелости; состояние сингулярности безопасности; предиктивное управление; когнитивная интеграция; рефлексивный контур; цифровая трансформация

Для цитирования. Ранверсман, А. Е. (2025). Состояние сингулярности безопасности: переход к рефлексивной системе обеспе-

чения транспортной безопасности. *Transportation and Information Technologies in Russia / Транспорт и информационные технологии*, *15*(4), 221–261. https://doi.org/10.12731/3033-5965-2025-15-4-385

Original article | Transport and Transport-Technological Systems

THE STATE OF SECURITY SINGULARITY: TRANSITION TOWARD A REFLEXIVE SYSTEM OF TRANSPORT SECURITY

A.E. Ranversman

Abstract

Background. The study substantiates the need to introduce a conceptual and model-based framework capable of capturing the evolutionary dynamics of the transport security system. The ongoing transformation of the transport sector is accompanied by changes affecting infrastructure, technical means and the distribution of functions between human and technological components, which leads to the emergence of new principles of security governance. In this context, there is a growing need for a maturity-level analytical model (C0-C5) that makes it possible to trace the trajectory of this evolution and identify the structural features of the transition from regulatory procedures to reflexive forms of management. The study also introduces the concept of the "state of security singularity" as the limit state of maturity of the transport security system, achieved through the shift toward self-regulation and the integration of technical means, analytical modules and human participation into a unified reflexive-integrated loop.

Purpose. The study aims to conceptualize the state of security singularity and to develop a maturity-level model (C0-C5) that reflects the transition from traditional organizational and regulatory procedures to intellectually adaptive mechanisms of threat pre-emption.

Materials and methods. The principal research method is modeling, which was used to develop the maturity-level model (C0-C5) and to con-

struct the reflexive-integrated loop governing the functioning of the transport security system.

The methodological foundation is based on a systemic and interdisciplinary approach, drawing upon theories of complex and sociotechnical systems, the cybernetic logic of security management, and a risk-oriented approach. The theoretical and regulatory basis of the study includes legal acts of the Russian Federation, ICAO and EASA documents, as well as strategic materials of the Ministry of Transport of the Russian Federation and the International Transport Forum. The research methods additionally include system-structural and normative-legal analysis, content analysis of strategic documents, and logic-prognostic (foresight) methods.

Results. The study proposes and theoretically grounds the concept of the "state of security singularity" as the limit state of maturity of the transport security system. It characterizes the stage at which the system reaches the level of self-reflection and self-regulation, where the mechanisms of response and threat prevention are based on a self-renewing risk management model, and the technical means, analytical modules and human participation are integrated into a unified reflexive-integrated loop. The maturity-level model (C0-C5) developed in the course of the research serves as the analytical framework for identifying the trajectory of this evolution and for assessing the degree of system readiness for further transitions. The obtained results can be used for diagnosing the level of system maturity, determining strategic directions of its development and defining competency requirements for security specialists under conditions of digital transformation.

Keywords: transport security; maturity-level model; state of security singularity; reflexive-integrated loop; self-renewing risk management; digital transformation; adaptive security architecture

For citation. Ranversman, A. E. (2025). The state of security singularity: transition toward a reflexive system of transport security. *Transportation and Information Technologies in Russia*, *15*(4), 221–261. https://doi.org/10.12731/3033-5965-2025-15-4-385

Введение

Развитие транспортного комплекса Российской Федерации на современном этапе ориентировано стратегическими приоритетами государственной политики, направленными на цифровую трансформацию, повышение технологической устойчивости и модернизацию механизмов обеспечения безопасности. В Стратегии научно-технологического развития Российской Федерации подчёркивается, что «большие вызовы создают существенные риски для общества, экономики, системы государственного управления, но одновременно представляют собой важный фактор для появления новых возможностей и перспектив научно-технологического развития» [1, п. 14]. Среди таких вызовов выделяются «новые гибридные внешние угрозы национальной безопасности, в том числе военные, террористические, информационные и биологические…» и «усиление их взаимосвязи с внутренними угрозами национальной безопасности» [1, п. 15, подп. ж]. Ответ на эти вызовы предполагает переход к новым технологическим и организационным моделям обеспечения безопасности. В том же документе указывается на необходимость перехода «к передовым технологиям проектирования и создания высокотехнологичной продукции, основанным на применении (…) результатов обработки больших объемов данных, технологий машинного обучения и искусственного интеллекта» [1, п.21, подп. а], а также на приоритет развития систем, ориентированных на «укрепление (…) национальной безопасности страны в условиях роста гибридных угроз» [1, п. 21, подп. д].

Таким образом, федеральный стратегический курс задаёт направление, в рамках которого система обеспечения безопасности транспортного комплекса постепенно приобретает способности к опережающему управлению рисками и адаптивности к условиям изменяющихся угроз.

На сегодняшний день в транспортной отрасли данные положения реализуются в том числе через механизмы цифровизации и ин-

теграции информационно-аналитических компонентов. В Докладе о реализации Транспортной стратегии Российской Федерации до 2030 года с прогнозом на период до 2035 года подчёркиваются развитие Единой государственной информационной системы обеспечения транспортной безопасности (ЕГИС ОТБ), внедрение интеллектуальных средств мониторинга и досмотра, оптимизация процессов обмена данными и повышение эффективности межведомственного взаимодействия [2]. Эти процессы формируют основу, задавая траекторию перехода от преимущественно регламентированного исполнения мер к управлению, основанному на анализе данных и оценке риска.

Однако темпы роста транспортных потоков дают основания предполагать, что текущая цифровая трансформация является лишь первым этапом адаптации системы к будущим условиям функционирования. Согласно долгосрочным прогнозам ICAO, мировой пассажирский авиапоток к 2045 году увеличится более чем в два раза по сравнению с докризисным периодом [3, с. 57]. Аналогичные тенденции представлены в ITF Transport Outlook 2023, где ожидается рост глобального пассажирского спроса на 79% к 2050 году и почти двукратное увеличение объёма грузовых перевозок [4, с. 15]. Расширение транспортной инфраструктуры и появление новых форм мобильности, включая беспилотные и аэромобильные системы, сопровождаются повышенными требованиями к устойчивости и адаптивности систем защиты. EASA отмечает, что ключевым условием общественного принятия аэромобильных систем является уровень безопасности, сопоставимый с авиационными стандартами [5, с. 73], что подтверждает определяющую роль факторов безопасности и управления рисками в устойчивом развитии новых транспортных технологий.

В этих условиях ключевое значение приобретает вопрос о предельных характеристиках развития системы обеспечения транспортной безопасности, связанный с пониманием того, каким образом может быть достигнута способность к опережающему

управлению рисками. В связи с этим в настоящем исследовании вводится понятие «состояние сингулярности безопасности» как предельного состояния зрелости системы обеспечения транспортной безопасности, чьё содержательное наполнение требует теоретического обоснования и дальнейшего раскрытия через модель уровней зрелости системы.

Цель настоящего исследования - теоретическое обоснование концепции состояния сингулярности безопасности и разработка модели уровней зрелости (C0-C5) системы обеспечения транспортной безопасности, отражающей переход от традиционных организационно-регламентированных процедур к интеллектуально-адаптивным механизмам упреждения угроз.

Материалы и методы

Методологической основой исследования является системный и междисциплинарный подход, в рамках которого обеспечение транспортной безопасности рассматривается как интегрированная социотехническая система, включающая правовые, организационные, инженерно-технические и информационно-аналитические компоненты. Теоретическая база исследования опирается на положения теории управления сложными системами, кибернетического подхода, концепции риск-ориентированного управления, а также идеи адаптивности, описывающие механизмы самоорганизации и устойчивости управляемых систем.

В качестве методологической опоры используются нормативные правовые акты Российской Федерации в сфере транспортной безопасности, международные документы ICAO и EASA, а также стратегические материалы Международного транспортного форума и Министерства транспорта Российской Федерации.

В исследовании применяются следующие методы:

– системно-структурный анализ, позволяющий рассматривать систему обеспечения транспортной безопасности как многоуровневую иерархическую структуру;

– нормативно-правовой и контент-анализ, используемые для реконструкции логики развития национальных и международных документов;
– моделирование, применяемое при разработке модели уровней зрелости (С0-С5) и построении рефлексивного контура функционирования системы;
– логико-прогностический метод, позволяющий определить возможную траекторию эволюции системы обеспечения транспортной безопасности в условиях цифровой трансформации.

Результаты и обсуждение

Эволюция теоретических и нормативных подходов к обеспечению транспортной безопасности

Система обеспечения транспортной безопасности в России формировалась как ответ на необходимость институционализации мер защиты объектов транспортного комплекса от актов незаконного вмешательства. На ранних этапах безопасность обеспечивалась в формате общей охранной деятельности и ведомственного контроля без единой системы выявления и предотвращения угроз и без самостоятельного института транспортной безопасности [6].

Институционализация отрасли началась с авиационного транспорта. Воздушным кодексом от 1997 года впервые была введена обязанность обеспечения авиационной безопасности как самостоятельной деятельности, отличной от общей охраны. На общетранспортный уровень регулирование было распространено в 2007 году с принятием Федерального закона № 16-ФЗ «О транспортной безопасности», который оформил единую систему, определил её участников, базовые понятия и порядок применения мер, введя нормативное определение обеспечения транспортной безопасности как «реализация определяемой государством системы правовых, экономических, организационных и иных мер в сфере

транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства» [7, п. 4, ст. 1].

С середины 2010-х годов развитие нормативной базы сопровождалось уточнением процедур категорирования объектов и оценки их уязвимости, а также дальнейшим упорядочением деятельности сил обеспечения транспортной безопасности. Данные изменения получили отражение в соответствующих методических рекомендациях для различных видов транспорта [8-11], что усилило формализованность процессов и повысило степень управляемости системы.

В настоящее время развитие международных подходов [12-14] ориентирует систему обеспечения транспортной безопасности на более высокий уровень информационной связности и аналитической поддержки принятия решений. В национальной практике эти тенденции проявляются через цифровизацию процессов и развитие ЕГИС ОТБ, что постепенно смещает акцент от разрозненной фиксации событий к их обработке и сопоставлению.

Таким образом, развитие нормативного регулирования и применение цифровых решений обеспечили институциональную зрелость системы, однако в условиях усложняющейся технологической среды механизм её функционирования определяется не только нормами, но и тем, каким образом между собой взаимодействуют уровни сбора, обработки и применения информации. Это требует её рассмотрения не только как правового института, но и как функционирующей модели с распределением ролей и уровней управления.

Структура действующей системы обеспечения транспортной безопасности с позиции кибернетики

В рамках системного и междисциплинарного подхода обеспечение транспортной безопасности рассматривается как совокупность правовых, организационных, инженерно-технических и информационно-аналитических компонентов, направленных на защиту объектов транспортной инфраструктуры и транспортных

средств от актов незаконного вмешательства. В качестве объекта системно-структурного анализа выступают нормативные и стратегические документы, определяющие порядок функционирования и траекторию развития системы обеспечения транспортной безопасности [2; 7; 15-24]. Анализ указанных источников позволяет реконструировать её функционирование как многоуровневую структуру, включающую:

- сенсорный уровень, на котором технические средства фиксируют исходные данные о событиях и параметрах контролируемой среды, обеспечивая их доступность для последующей интерпретации исполнителями;
- аналитический уровень, на котором осуществляется интерпретация поступающих данных и оценка риска. В действующей модели он имеет человекоцентричный характер и реализуется на трёх плоскостях: (1) на операционном уровне - работниками подразделений транспортной безопасности через ситуативную оценку при осуществлении мер защиты; (2) на уровне субъекта транспортной инфраструктуры - через систематизацию и передачу информации по установленным каналам; (3) на федеральном уровне - через обобщение и интерпретацию поступающих сведений, результаты которых служат основанием для корректировки нормативного регулирования;
- стратегический уровень, на котором результаты агрегированной аналитики преобразуются в управленческие решения: (1) на федеральном уровне - через их отражение в нормативном регулировании; (2) на уровне субъекта транспортной инфраструктуры - через организационные и процедурные решения по реализации установленных норм и требований.

С позиций кибернетической теории управления система обеспечения транспортной безопасности представляет собой иерархическую многоуровневую структуру с элементами об-

ратной связи. В классическом понимании кибернетики эффективность функционирования любой системы определяется степенью замкнутости информационных контуров и способностью преобразовывать внешние возмущения в корректирующие действия [25; 26].

Применительно к транспортной безопасности это означает, что устойчивость системы определяется не только наличием сенсорных данных, но и скоростью возврата результатов проанализированных данных в управленческий контур, позволяя корректировать меры защиты. В идеальной кибернетической модели между этими уровнями формируются замкнутые обратные связи, при которых управленческие решения на стратегическом уровне определяют нормативную и организационную конфигурацию функционирования системы, влияющую на работу сенсорного и аналитического уровней, а те, в свою очередь, обеспечивают возврат актуализированных данных в управляющий контур. Такая взаимосвязанность обеспечивает адаптивность и предиктивность системы – способность не только реагировать на угрозы, но и прогнозировать их развитие.

На основе сопоставления идеальной кибернетической модели с действующей практикой функционирования системы обеспечения транспортной безопасности становится возможным сделать вывод, что реальное её исполнение характеризуется преобладанием управленческого контура, тогда как обратная связь между анализом данных и управленческим возвратом решения остаётся частично разомкнутой. Информационный обмен в установленных процедурах носит преимущественно отчётный характер, и переработанные сведения не всегда оперативно трансформируются в корректировку применяемых мер, что снижает способность системы к быстрой адаптации и упреждающему реагированию на изменение характера угроз. Устранение указанного разрыва возможно за счёт усиления предиктивных и адаптивных механизмов управления.

Концепции предиктивного
и адаптивного управления безопасностью

В современных условиях цифровой трансформации обеспечение безопасности становится затруднительным без прогнозирования и динамической коррекции управленческих решений. Это связано с тем, что технологическое развитие и усложнение угроз происходят быстрее, чем обновляются организационно-правовые механизмы реагирования. Указанные условия предопределяют обращение к концепциям предиктивного и адаптивного управления безопасностью, которые формируют переходный этап от регламентированной к рефлексивной модели функционирования системы.

Предиктивное управление безопасностью (от англ. predictive security management) основано на упреждающем выявлении потенциальных угроз и рисков до момента их реализации. В международной практике его ключевые принципы концептуально соотносятся с глобальными приоритетами ICAO, сформулированными в Global Aviation Security Plan (в части повышения осведомлённости о рисках и упреждающего реагирования) [12, с. 16], а также с выводами ITF Transport Outlook 2023, где подчёркивается, что «Demand for passenger and freight transport will continue to grow in the coming decades across all world regions, regardless of the scenario» («Спрос на пассажирские и грузовые перевозки будет продолжать расти в предстоящие десятилетия во всех мировых регионах вне зависимости от сценария») [4, с. 74], что объективно усиливает необходимость более раннего принятия управленческих решений и прогнозно-ориентированного управления. Содержательно данный подход предполагает интеграцию данных, поступающих от технических средств и внешних источников аналитической информации в единый механизм прогнозирования риска.

В обобщённом виде принципы предиктивного управления могут быть представлены следующим образом:

– постоянный мониторинг и анализ динамических параметров среды;

– использование методов машинного обучения и искусственного интеллекта для прогнозирования рисков;
– ранжирование угроз по вероятности и критичности последствий;
– реализация упреждающих мер защиты без ожидания наступления события.

Применительно к транспортной безопасности предиктивный подход обеспечивает переход от фиксированных регламентов к риск-ориентированным сценариям реагирования и способствует формированию интеллектуальных систем поддержки решений.

Адаптивное управление безопасностью является развитием предиктивного подхода и направлено на поддержание устойчивости системы при изменяющихся внешних условиях. Его методологическая основа восходит к общей теории систем и идеям самоорганизующегося поведения сложных систем [27-30]. В отличие от предиктивного управления, ориентированного на упреждающее обнаружение угроз, адаптивное управление обеспечивает динамическую перенастройку системы в зависимости от текущего уровня риска и контекста событий. В обобщённом виде к его характерным принципам относятся:

– наличие механизма непрерывной обратной связи между сенсорным, аналитическим и стратегическим уровнями;
– самообучение системы на основе накопленных данных о нарушениях и результатах реагирования;
– перераспределение ресурсов и приоритетов в зависимости от контекста ситуации;
– динамическая оптимизация мер защиты с учётом вероятностной оценки риска.

Реализация адаптивного управления предполагает усиление интеллектуальных модулей анализа и корректировки мер защиты на основе текущих параметров риска, а также более глубокую интеграцию информационно-аналитических платформ и данных от технических средств обеспечения транспортной безопасности. В

нормативно-стратегическом контексте данная логика развития отражена в Транспортной стратегии Российской Федерации до 2030 года с прогнозом до 2035 года, где в числе приоритетов обозначается развитие интеллектуальных транспортных систем и расширение применения цифровых технологий.

Таким образом, концепции предиктивного и адаптивного управления образуют взаимосвязанный контур развития системы обеспечения транспортной безопасности: первая обеспечивает упреждающее прогнозирование угроз, вторая – адаптацию к изменяющимся условиям. Их сочетание формирует методологическую основу рефлексивной модели, характеризующейся когнитивной интеграцией человека, технологий и нормативной среды и создаёт теоретические предпосылки для разработки модели уровней зрелости системы обеспечения транспортной безопасности.

Сущность и категориальные признаки состояния сингулярности безопасности

Понятие «сингулярность» в строгом научном смысле сформировалось в математике. В современном математическом подходе сингулярность описывается как состояние, при котором объект перестаёт соответствовать нормальному (регулярному) режиму описания. Как указывают Г.-М. Гройль, К. Лоссен и Е. Шустин, «… singularities … always refer to a situation which is not regular, that is, not the usual, or expected, one» («…сингулярности… всегда относятся к ситуации, которая не является регулярной, то есть выходит за пределы обычного или ожидаемого состояния») [31, с. 1].

В классической кибернетике зарождение категории сингулярности связано с развитием идеи замкнутого контура саморегулирования, при котором система перестаёт быть объектом внешнего управления и приобретает способность поддерживать собственные параметры функционирования. У Н. Виннера эта логика впервые была описана через принцип автономного поддержания состояния системы: «There are, however, feedback chains in which no

human element intervenes» («Однако существуют такие контуры обратной связи, в которых участие человека отсутствует.») [25, с. 131]. Этот пример является исходной формой саморегуляции, из которой в последующем развивается концепция предельных состояний управляемых систем.

Дальнейшее развитие эта логика получила у У.Р. Эшби, который связывает предельное состояние управляемой системы с её способностью самостоятельно изменять собственную организацию в ответ на нарушение устойчивости. Описывая механизм ультраустойчивости, Эшби фиксирует не просто реакцию на воздействие среды, а поиск системой такого внутреннего состояния, при котором корректировка перестает требовать внешнего управляющего воздействия. Этот процесс он объясняет следующим образом: «If the field leads the point to a critical state, a step-function will change value and the field will be changed. If the new field again leads the point to a critical state, again a step-function will change and again the field will be changed; and so on. The two factors, then, generate a process» («Если поле приводит точку к критическому состоянию, шаг-функция изменяет своё значение и тем самым изменяет поле. Если новое поле снова приводит точку к критическому состоянию, шаг-функция вновь изменяется, и поле снова меняется; и так далее. Таким образом эти два фактора порождают процесс») [26, с. 91].

Далее он уточняет, что результатом такого процесса становится избирательное удержание устойчивых состояний: «… an ultrastable system acts selectively towards the fields of the main variables, rejecting those that lead the representative point to a critical state but retaining those that do not» («…ультраустойчивая система действует избирательно по отношению к возможным полям основных переменных: отклоняющие её в критическое состояние отбрасываются, а не приводящие к критическим состояниям – сохраняются») [26, с. 91].

Тем самым Эшби формализует переход от адаптации как внешнего исправления к самонастройке как внутреннему свойству систе-

мы – именно это концептуально лежит в основании будущей категории сингулярности как предельного состояния управляемой системы.

В советской школе кибернетики идея предельного состояния системы, в котором управление перестаёт быть внешним и становится внутренне присущим свойством самой системы, была концептуально сформулирована в работе А. А. Соболева, А. И. Китова и А. А. Ляпунова «Кибернетика - общие черты» [32]. Авторы показали, что высший уровень развития управляемой системы связан с переходом от внешнего регулирования к такому режиму, при котором система изменяет собственные параметры и алгоритм функционирования, опираясь на результаты собственной работы и механизм обратной связи. Иными словами, корректирующее воздействие перестаёт поступать извне и становится частью внутреннего контура функционирования системы.

Таким образом, высший этап развития управляемой системы можно охарактеризовать как состояние, при котором механизм регулирования превращается во внутреннее свойство самой системы. Система не только реагирует на внешние воздействия, но и самостоятельно перестраивает собственные параметры и алгоритм функционирования на основе результатов собственной работы.

Перенос данной логики в сферу транспортной безопасности возможен ввиду того, что современные технические средства обеспечения транспортной безопасности уже обладают отдельными признаками кибернетических систем, включающих элементы обратной связи. Они фиксируют параметры контролируемого объекта, осуществляют их первичную интерпретацию и сигнализируют о наличии потенциального отклонения (например, выделение зоны интереса на рентгенотелевизионном изображении, подача тревожного сигнала стационарным металлоискателем или детектором паров взрывчатых веществ). При этом формирование решения о применении мер воздействия остаётся внешним по отношению к технологическому контуру и осуществляется работником подразделения транспортной безопасности. Таким образом, тех-

нологический контур уже приобретает элементы предиктивности, однако полный цикл – от обнаружения к выбору и инициированию реагирования – остаётся незамкнутым и составляет границу перехода к состоянию сингулярности безопасности.

В данном исследовании *состояние сингулярности безопасности* представляет собой *предельное состояние зрелости системы обеспечения транспортной безопасности, при котором она достигает уровня саморефлексии и саморегуляции, когда механизмы реагирования и предотвращения угроз основаны на непрерывной самообновляемой модели управления рисками, а технические средства, аналитические модули и человеческое участие объединяются в единый рефлексивный контур*.

При этом важно подчеркнуть, что состояние сингулярности безопасности не тождественно технологической сингулярности. В последнем случае акцент смещается на автономизацию алгоритмов и утрату контроля со стороны человека, тогда как в системе обеспечения транспортной безопасности сохраняется обязательное участие работника, выполняющего функцию носителя правовой и ситуационной ответственности. Таким образом, сингулярность безопасности означает не отказ от человеческого участия, а его трансформацию – от операционной деятельности к когнитивно-аналитической.

Категориальные признаки состояния сингулярности безопасности могут быть представлены в следующем виде:

- целостность информационно-управленческого цикла, обеспечивающего замкнутость обратных связей;
- способность системы к самообновлению процедур реагирования на основе анализа накопленных данных;
- переход от статических алгоритмов контроля к динамически формируемым сценариям безопасности;
- интеграция технических, аналитических и организационных контуров в единую рефлексивную логику функционирования;

– смещение роли работника от оператора технических систем к интерпретатору данных и модератору управленческих решений;
– опережающий характер реагирования, основанный на прогнозной модели оценки риска.

Перечисленные признаки формируют основание для последующей операционализации сингулярности безопасности через модель уровней зрелости системы обеспечения транспортной безопасности (C0-C5), в которой состояние сингулярности будет выступать предельным уровнем зрелости развития системы (уровень C5).

Модель и структурное описание уровней зрелости системы обеспечения транспортной безопасности (C0-C5)

Для того чтобы отразить движение системы обеспечения транспортной безопасности от текущего состояния к предельному уровню зрелости, необходим инструмент, позволяющий зафиксировать промежуточные стадии её развития. Модель, отражающая данную траекторию, представлена в виде последовательности уровней зрелости (C0-C5) системы.

Поскольку модель представлена в ступенчатой визуально-структурной форме (матрица уровней и графическая схема), её внешнее восприятие может быть сопоставлено с известными maturity-подходами (CMMI, ISO/IEC 330xx (SPICE), BPMM, ITIL, COBIT, OPM3). Однако сходство ограничивается исключительно формой представления, тогда как содержательно данный инструмент фиксирует не степень формализованности процессов, а изменение самой логики функционирования системы и источника инициирования реагирования – от организационно-регламентированной логики управления к рефлексивной (саморегулируемой) среде, в которой упреждение угроз становится внутренним свойством системы.

Для операционализации данной логики далее приводится концептуальная матрица уровней зрелости (C0-C5), задающая структурные признаки переходов между состояниями системы (Таблица 1).

Таблица 1.

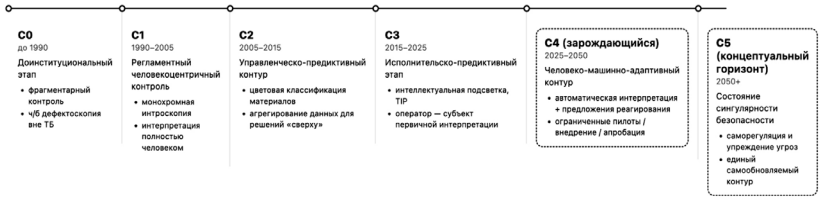
Матрица уровней зрелости системы обеспечения транспортной безопасности (С0–С5)

Уровень	Тип управленческого контура	Функциональная роль работника ПТБ	Уровень интеграции данных	Модель реагирования
С0 доинституциональный	отсутствует	отсутствует (институт не сформирован)	данные не собираются системно	реагирование постфактум, эпизодическое
С1 регламентный	нормативно-регламентированный	исполнитель в пределах полномочий	разрозненные данные, отчётный характер	реагирование по факту, по алгоритму
С2 управленческо-предиктивный	управленческо-предиктивный	исполнитель без самостоятельной риск-интерпретации	агрегированные данные для управленческих решений	упреждающее реагирование по указанию руководства
С3 исполнительско-предиктивный	исполнительско-предиктивный	исполнитель как субъект первичной интерпретации риска	сквозная интеграция данных для опоры на собственную оценку	упреждающее реагирование по инициативе исполнителя
С4 адаптивный	человеко-машинно-адаптивный	верификатор и модератор предложений системы	автоматическая интерпретация данных и предварительная классификация угроз	адаптивное реагирование в режиме реального времени
С5 состояние сингулярности безопасности	рефлексивный (саморегулируемый)	когнитивный надзор за системой	единый самообновляемый контур	рефлексивная саморегуляция и упреждение

Перечисленные уровни отражают не только логическую, но и технологическую динамику развития системы обеспечения транспортной безопасности. При этом важно отметить, что в реальной практике отрасль находится в переходной зоне между уровнями С2-С3, тогда как элементы С4 присутствуют лишь точечно – в фор-

мате пилотных решений и отдельных технологических внедрений. Уровень С5 рассматривается как предельный этап зрелости, имеющий концептуальный характер.

Для демонстрации этой динамики уместно представить модель уровней зрелости в виде временной последовательности, отражающей переход от исторически сложившихся форм контроля к рефлексивной форме управления и интеллектуально-адаптивным механизмам упреждения угроз (рисунок 1). При этом важно подчеркнуть, что временная шкала сформирована на основе мировой технологической эволюции, поскольку именно она наиболее полно отображает логику смены уровней. Национальное развитие соотносится с этой шкалой не по календарным датам, а по достигнутому уровню зрелости и фактической глубине применения технологий.



Примечание. Временные рамки отражают международную эволюцию технологий; в национальных практиках возможно отставание внедрения. Уровни С4–С5 — целевая траектория, не доминирующая на текущем этапе.

Рис. 1. Временная шкала модели уровней зрелости системы

Для наглядности дальнейшее изложение структуры уровней зрелости представлено последовательно - от начального состояния (С0) к предельному (С5). Каждый уровень фиксирует качественные изменения в механизмах управления, роли работника подразделения транспортной безопасности, характере обработки данных и модели реагирования. Ниже приводится их содержательное описание.

Уровень С0 - доинституциональный

Уровень С0 характеризует состояние, предшествующее формированию системы обеспечения транспортной безопасности

как самостоятельного института. Управление транспортной безопасностью на данном этапе носит фрагментарный и преимущественно реактивный характер, опираясь не на систему управления рисками, а на общие меры охраны объектов и контроля доступа. Технические средства обеспечения транспортной безопасности отсутствуют либо используются эпизодически и не встраиваются в единую информационную среду. Обработка данных не осуществляется в системном режиме, что исключает возможность аналитики и прогнозирования. Работник подразделения транспортной безопасности как профессиональная единица не присутствует, поскольку соответствующая функция ещё не институционализирована. Реагирование на угрозы осуществляется по факту их проявления и не носит упреждающего или адаптивного характера.

Уровень С1 - регламентный

Уровень С1 отражает этап, на котором система обеспечения транспортной безопасности функционирует исключительно в рамках предписанных процедур и алгоритмов реагирования. Распознавание угрозы происходит только после её проявления, а действия работника подразделения транспортной безопасности носят реактивный характер. Функциональная роль работника ограничивается исполнением регламентированных действий в пределах установленных полномочий. Принятие решения происходит не в результате оценочной деятельности, а в силу наступления формально определённого события (например, срабатывания технического средства или выявления факта нарушения). Информация о происшествиях фиксируется и передаётся для последующего анализа, однако результаты этого анализа возвращаются в систему лишь через нормативно установленные изменения и не преобразуются в оперативно доступный механизм превентивного управления. На данном уровне отсутствует самостоятельная интерпретация риска, а реагирование осуществляется постфактум, строго в соответствии с закреплёнными алгоритмами.

Уровень С2 – управленческо-предиктивный

На уровне С2 упреждение угроз реализуется через управленческие решения, поступающие сверху и доводимые до исполнителей руководством подразделения. Руководитель не формирует прогноз самостоятельно, а транслирует полученную информацию и связанные с ней меры, такие как введение усиленных мер защиты, изменение уровня безопасности или установление дополнительных требований к досмотру. Исполнитель по-прежнему действует в рамках регламентированных процедур, однако реагирование инициируется не фактом наступления события (как на уровне С1), а поступившим управленческим сигналом. Предиктивность на данном этапе носит централизованный характер и выражается в том, что система начинает реагировать упреждающе, хотя инициатива остаётся на стороне вышестоящего звена.

Уровень С3 – исполнительско-предиктивный

На уровне С3 способность к предвосхищению угроз появляется на уровне исполнителя. Работник подразделения транспортной безопасности принимает решение о применении мер усиленного контроля не только после наступления события и не в результате управленческого решения, а исходя из самостоятельной оценки складывающейся обстановки. Основанием для такого решения становятся наблюдаемое поведение лица, особенности его действий, несоответствие намерений и контекста ситуации, а также совокупность внешних признаков, свидетельствующих о возможном риске. Впервые появляется возможность упреждающего реагирования «на месте», когда инициатива запуска мер исходит от исполнителя. Руководитель сохраняет координирующую и подтверждающую роль, однако исходная точка распознавания риска смещается на уровень непосредственного исполнителя, что отражает переход от строго регламентированной модели к модели, включающей элементы самостоятельной оценочной деятельности.

Уровень С4 – человеко-машинно-адаптивный

На данном уровне первичное распознавание и предварительная классификация угроз осуществляется техническими средствами и информационными системами, способными автоматически интерпретировать поступающие данные и определять вероятность наличия риска. Система не ограничивается сигнализацией факта отклонения, а формирует предложение по реагированию, которое подтверждается или корректируется работником подразделения транспортной безопасности. Человек остаётся носителем итогового управленческого решения, однако инициирующее звено смещается от исполнителя к технологическому контуру, что обеспечивает адаптивность реагирования и сокращает временной разрыв между моментом выявления потенциальной угрозы и началом применения мер по защите.

Уровень С5 - состояние сингулярности безопасности

Уровень С5 представляет предельную стадию зрелости системы обеспечения транспортной безопасности, при которой механизм предотвращения угроз становится саморегулируемым и действует упреждающе не только во временном, но и в пространственном отношении. В отличие от предыдущих уровней, где инициатива реагирования принадлежит либо руководящему звену, либо исполнителю, на уровне С5 исходная точка принятия решения смещается в технологический контур: система самостоятельно выявляет, интерпретирует и инициирует применение мер до момента соприкосновения потенциального нарушителя с рубежами контроля.

Ключевым отличием данного уровня является перенос фильтрации угроз за пределы точки досмотра, в так называемую зону предварительного упреждения, что позволяет не допускать концентрации рисков в области непосредственного контроля и сохранять пропускную способность объекта транспортной инфраструктуры. Перераспределение пассажиропотока либо перевод отдельных лиц в зоны углублённого контроля осуществляется автоматически на ос-

нове динамической конфигурации параметров безопасности, формируемой системой в режиме реального времени.

На этом уровне участие работника подразделения транспортной безопасности носит характер когнитивного надзора и выражается не в инициировании реагирования, а в проверке корректности исполнения автоматически сформированных системой решений в сложных или неоднозначных ситуациях, когда требуется экспертное толкование конкретных обстоятельств. Доступ к информации о потенциальных рисках обеспечивается через расширенные визуальные интерфейсы (AR/VR-очки, ситуационные панели, когнитивные терминалы), позволяющие получать не только сигнал о наличии потенциальной угрозы, но и видеть предшествующую динамику – изменение параметров потока, особенности траектории перемещения и другие индикаторы риска.

В конечном виде уровень С5 характеризует переход к саморефлексивной модели безопасности, в которой предотвращение угроз становится внутренним свойством системы, а не реакцией на внешнее событие. Отличительной чертой является не только автоматическое выявление и инициация мер защиты, но и способность системы пересматривать собственные параметры функционирования в реальном времени, обеспечивая устойчивость к изменению профиля угроз без остановки процессов и без снижения пропускной способности. Человек сохраняется в контуре управления как гарант правомерности и корректности применения мер безопасности, однако его участие носит надсистемный характер и направлено на поддержание доверия и легитимности работы технологического контура. Тем самым сингулярность безопасности представляет собой состояние, при котором система обладает свойством самонастройки, самоподдержания и упреждающего предотвращения рисков без необходимости инициирования реагирования со стороны человека.

Эволюция системы обеспечения транспортной безопасности представлена в виде ступенчатой модели уровней зрелости

(C0-C5), отражающей переход от доинституционального состояния к предельному уровню, при котором управление приобретает рефлексивный характер. Блок-схема иллюстрирует изменение источника инициирования реагирования: от традиционных организационно-регламентированных процедур к интеллектуально-адаптивным механизмам упреждения угроз.

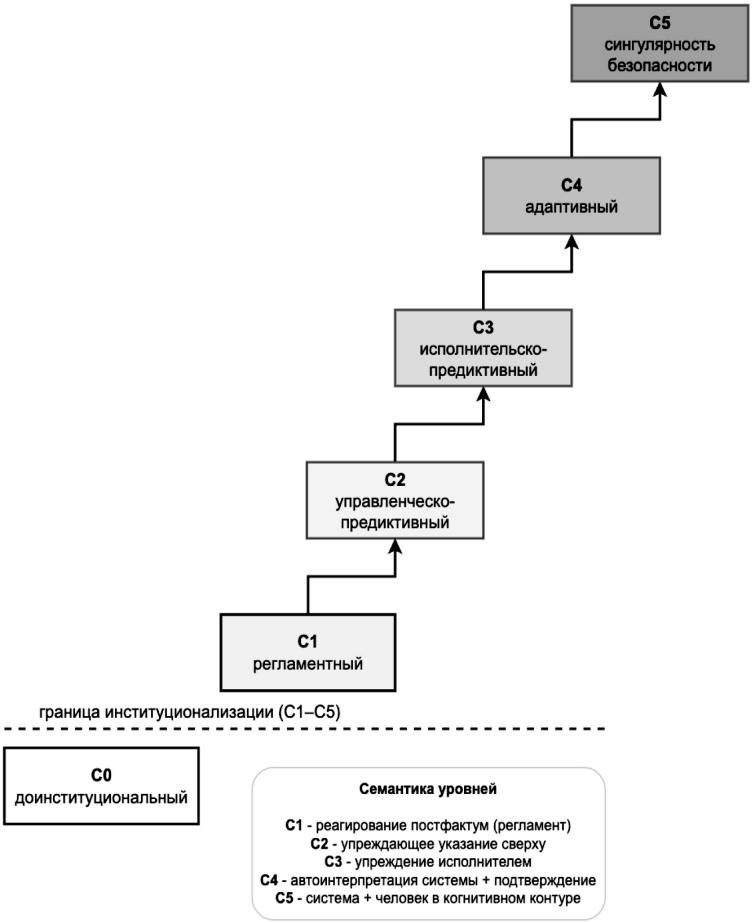


Рис. 2. Блок-схема модели уровней зрелости системы обеспечения транспортной безопасности (C0–C5)

Для того чтобы диагностировать не только уровень участия человека в принятии решений, но и степень технологической оснащённости системы, модель зрелости должна рассматриваться в двух взаимосвязанных контурах – человеческом и техническом. Первый отражает распределение субъектности и инициативы в реагировании, второй – глубину и характер выявления угроз техническими средствами. Однако на практике развитие системы обеспечения транспортной безопасности связано не только с технологическими и когнитивными изменениями, но и с эволюцией управленческой архитектуры, определяющей, каким образом решения возникают и распространяются внутри системы.

Поэтому зрелость системы проявляется одновременно в трёх контурах:

– техническом (уровень автономности выявления угроз),
– информационно-аналитическом (глубина обработки и интерпретации данных),
– организационно-нормативном (характер управленческого цикла и распределение инициативы).

Именно сочетание этих трёх контуров позволяет объективно определить, на какой стадии развития находится система и насколько она приближается к состоянию сингулярности безопасности. Сводная оценка представлена в таблице 2.

Таблица 2.

Индикаторы проявления уровней зрелости (C0–C5) с учётом роли исполнителя и технических средств

Блок	Критерии	Индикатор проявления (с примерами)	Уровень модели	Роль исполнителя
(предсистемный уровень)			C0	Профессиональный субъект ещё отсутствует (функция не институционализирована)

Технический	Степень автономности первичного выявления угроз	Средства фиксируют факт наличия потенциально опасного объекта без участия работника (пример: стационарный металлоискатель (рамка) подаёт сигнал, если обнаружен металл)	C2	Исполнитель реагирует только после сигнала, без интерпретации
	Адресное указание зоны внимания	Система не только сигнализирует, но и локализует предполагаемую область риска (пример: радиоскопическая установка (портал) или рентгенотелевизионная установка (интроскоп) выделяет «зону интереса»)	C3	Исполнитель использует локализацию для оценки и инициирует реагирование
	Автоматизация интерпретации	Алгоритм не просто фиксирует, но классифицирует объект (пример: интеллектуальные интроскопы нового поколения, определяющие тип предмета — «жидкость», «нож», «оружие», и предлагающие меру реагирования)	C4	Исполнитель подтверждает или корректирует решение системы
	Пространственно-упреждающее предотвращение	Система перераспределяет потоки до точки контроля, автоматически перенаправляя риск-субъектов (пример: интеллектуальная перенастройка маршрута до входа в зону досмотра)	C5	Исполнитель в роли когнитивного надзора

Информационно-аналитический	Тип обрабатываемых данных	Используется совокупность признаков, а не единичное срабатывание (пример: видеоаналитика отслеживает траекторию перемещения лица, сопоставляя несколько параметров поведения)	С3	Исполнитель дополняет технический сигнал контекстной оценкой и инициирует реагирование «на месте»
	Интеграция источников данных	Данные от разных технических средств объединяются в единый аналитический контур (пример: система сопоставляет данные от интроскопа и портала без участия человека)	С4	Исполнитель выполняет адаптивно-корректирующую роль (подтверждает или корректирует решение системы)
	Формат представления информации	Применяются когнитивные интерфейсы (AR/VR, ситуационные панели), обеспечивающие динамическую картину риска	С5	Исполнитель осуществляет когнитивный надзор: подключается только при неоднозначности результата
	Характер управленческого уровня	Управление строится по схеме: «событие > фиксация > передача > последующее решение». Корректировка всегда запаздывает	С1	Исполнитель действует строго по регламенту, без оценочной деятельности
	Источник инициирования изменений	Решение о введении мер (усиление контроля, изменение уровня безопасности) исходит исключительно сверху и доводится до исполнителя через руководство	С2	Исполнитель исключительно исполняет управленческое решение, не участвует в его формировании

Организационно-нормативный	Локальная инициатива	Допускается упреждающее реагирование на месте в пределах полномочий исполнителя	С3	Исполнитель впервые становится инициатором применения мер до внешнего распоряжения
	Динамичность и адаптивность	Корректировка мер происходит в процессе функционирования, а не постфактум	С4	Исполнитель выполняет адаптивную функцию - подтверждает/корректирует решение, порождаемое системой
	Предиктивность организационной среды	Управленческие механизмы работают упреждающе, меры конфигурируются до входа угрозы в зону контроля	С5	Исполнитель выполняет надзорную (когнитивную) функцию, а не операционную

Примечание: стационарные и ручные металлоискатели и иные устройства сигнализационного типа относятся к уровню С2, поскольку фиксируют единичный признак и не выполняют аналитическую интерпретацию риска. Они не могут быть отнесены к уровню С3, так как не обеспечивают распознавания устойчивых поведенческих или корреляционных признаков угрозы.

Таким образом, представленная модель демонстрирует, что развитие системы обеспечения транспортной безопасности не сводится к модернизации технических средств, а представляет собой последовательную трансформацию распределения субъектности между человеком и технологическим контуром. Сдвиг от реактивного исполнения к упреждающему реагированию, а затем –

к когнитивному надзору отражает переход от организационно-регламентированной системы к самонастраивающейся среде безопасности. Это создаёт методологические основания для оценки степени зрелости системы и позволяет выявить условия, при которых возможно достижение состояния сингулярности безопасности.

Заключение

Проведённое исследование позволило обосновать концептуальный переход от традиционной регламентной модели обеспечения транспортной безопасности к модели уровней зрелости (C0-C5), в которой состояние сингулярности безопасности понимается как предельное состояние зрелости системы обеспечения транспортной безопасности, при котором она достигает уровня саморефлексии и саморегуляции, когда механизмы реагирования и предотвращения угроз основаны на непрерывной самообновляемой модели управления рисками, а технические средства, аналитические модули и человеческое участие объединяются в единый рефлексивный контур.

Разработанная модель показывает, что движение к состоянию сингулярности безопасности носит поступательный характер и предполагает последовательное перераспределение инициативы внутри системы: от нормативно установленного реагирования (C1) и управленческого упреждения угроз (C2) – к субъектности исполнителя при принятии решений (C3), далее к технологически инициируемому реагированию в связке «человек-машина» (C4) и, наконец, к когнитивному надзору в условиях саморегулируемого контура (C5), где человек сохраняет надсистемную функцию контроля правомерности и легитимности решений. Таким образом, достижение состояния сингулярности безопасности выступает не как одномоментный скачок, а как логический результат эволюционного усложнения механизмов управления рисками.

Полученные результаты могут быть использованы для диагностики уровня зрелости системы, определения направления её

дальнейшей эволюции и обоснования требований к подготовке специалистов в условиях цифровой трансформации.

Развитие системы обеспечения транспортной безопасности в логике представленной модели требует переосмысления роли человека и механизмов нормативного регулирования. По мере приближения к адаптивным и рефлексивным уровням (С4-С5) меняется характер участия работника: от операционного исполнения – к аналитической интерпретации данных и контролю корректности функционирования технологического контура. Это, в свою очередь, предполагает смещение акцента подготовки с процедурных навыков на когнитивные и прогностические компетенции, связанные с оценкой риска, ситуационным анализом и подтверждением правомерности автоматизированных решений, а также поэтапную эволюцию нормативно-технической базы в сторону включения механизмов цифровой поддержки и упреждающего реагирования.

Дальнейшее развитие данной линии исследования связано с определением условий достижения уровня С5 в реальной практике, которые включают требования к профессиональной подготовке работников, обновлению нормативной базы, а также уточнение структуры взаимосвязи технических и аналитических систем. Это задаёт направление для последующих исследований, ориентированных на переход от концептуальной модели к операционализации принципов состояния сингулярности безопасности в отраслевой практике.

Список литературы

1. Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации» (2024). Получено с официального интернет-портала правовой информации.
2. Доклад о реализации Транспортной стратегии Российской Федерации до 2030 года с прогнозом на период до 2035 года (2025). Получено с официального интернет-портала Министерства транспорта Российской Федерации.

3. Международная организация гражданской авиации (2019). *Aviation Benefits Report 2019*. Монреаль: ИКАО. Получено с: https://icao.assyst-uc.com/sites/default/files/sp-files/sustainability/Documents/AVIATION-BENEFITS-2019-web.pdf (дата обращения: 16 октября 2025 г.).
4. Международный транспортный форум (2023). *ITF Transport Outlook 2023*. Париж: OECD/ITF. https://doi.org/10.1787/b6cc9ad5-en
5. Европейское агентство по авиационной безопасности (2021). *Study on the Societal Acceptance of Urban Air Mobility in Europe*. Cologne: EASA. Получено с: https://www.easa.europa.eu/sites/default/files/dfu/uam-full-report.pdf (дата обращения: 16 октября 2025 г.).
6. Попов, Е. А., Штырхунова, Н. А., & Абрамян, С. К. (2021). Эволюция транспортной безопасности в России. *Гуманитарные, социально-экономические и общественные науки*, (4-2), 126–128. https://doi.org/10.23672/x7501-1481-8798-n. EDN: https://elibrary.ru/RGBUHA
7. Федеральный закон № 16-ФЗ от 9 февраля 2007 г. «О транспортной безопасности» (2007). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_66069/ (дата обращения: 16 октября 2025 г.).
8. ГОСТ Р 57119-2016. *Методика проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств. Общие требования* (2019). Москва: Стандартинформ, 18 с.
9. Распоряжение Федерального дорожного агентства от 10 ноября 2014 г. № 2159-р «Об издании и применении ОДМ 218.6.013-2014 „Методические рекомендации по разработке планов обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств городского наземного электрического транспорта“» (2014). Получено с официального интернет-портала Федерального дорожного агентства Росавтодор: https://rosavtodor.gov.ru/docs/prikazy-rasporyazheniya/12717 (дата обращения: 16 октября 2025 г.).

10. Распоряжение Росавтодора от 15 ноября 2011 г. № 871-р «Об издании и применении ОДМ 218.4.007-2011 „Методические рекомендации по проведению оценки уязвимости объектов транспортной инфраструктуры в сфере дорожного хозяйства“ (вместе с „ОДМ 218.4.007-2011. Отраслевой дорожный методический документ“)» (2011). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_125293/ (дата обращения: 16 октября 2025 г.).
11. Приказ Росжелдора от 7 марта 2013 г. № 73 «Об отмене приказа Росжелдора от 25 октября 2011 г. № 515 „Об утверждении Методических рекомендаций по проведению оценки уязвимости объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта“» (2013). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_145508/ (дата обращения: 16 октября 2025 г.).
12. Международная организация гражданской авиации (2024). *Global Aviation Security Plan*. Монреаль: ИКАО. Получено с: https://www.icao.int/sites/default/files/sp-files/Security/Documents/GLOBAL AVIATION SECURITY PLAN 2nd Ed.RU.pdf (дата обращения: 16 октября 2025 г.).
13. Международная организация гражданской авиации (2017). *Aviation Security Manual* (Doc 8973) (10-е изд.). Монреаль: ИКАО. ISBN: 978-92-9258-277-7
14. Европейское агентство по авиационной безопасности (2023). *Artificial Intelligence Roadmap 2.0. A Human-Centric Approach to AI in Aviation*. Cologne: EASA. Получено с: https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20 (дата обращения: 16 октября 2025 г.).
15. Постановление Правительства Российской Федерации от 5 октября 2020 г. № 1605 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищённости объектов (территорий), учитывающих уровни безопасности для различных категорий объектов

транспортной инфраструктуры воздушного транспорта» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_364707/ (дата обращения: 16 октября 2025 г.).

16. Постановление Правительства Российской Федерации от 8 октября 2020 г. № 1633 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищённости объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры железнодорожного транспорта» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_365316/ (дата обращения: 16 октября 2025 г.).
17. Постановление Правительства Российской Федерации от 8 октября 2020 г. № 1637 «Об утверждении требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для транспортных средств морского и внутреннего водного транспорта» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_364993/ (дата обращения: 16 октября 2025 г.).
18. Постановление Правительства Российской Федерации от 8 октября 2020 г. № 1638 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищённости объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры морского и речного транспорта» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_364994/ (дата обращения: 16 октября 2025 г.).
19. Постановление Правительства Российской Федерации от 8 октября 2020 г. № 1640 «Об утверждении требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для транспортных средств автомобильного транспорта и город-

ского наземного электрического транспорта» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_364995/ (дата обращения: 16 октября 2025 г.).

20. Постановление Правительства Российской Федерации от 8 октября 2020 г. № 1641 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищённости объектов (территорий), учитывающих уровни безопасности для различных категорий объектов инфраструктуры внеуличного транспорта (в части метрополитенов)» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_365322/ (дата обращения: 16 октября 2025 г.).
21. Постановление Правительства Российской Федерации от 8 октября 2020 г. № 1642 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищённости объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры автомобильного транспорта» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_365313/ (дата обращения: 16 октября 2025 г.).
22. Постановление Правительства Российской Федерации от 21 декабря 2020 г. № 2201 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищённости объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры дорожного хозяйства» (2020). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_371982/ (дата обращения: 16 октября 2025 г.).
23. Распоряжение Правительства Российской Федерации от 27 ноября 2021 г. № 3363-р «О Транспортной стратегии Российской Федерации до 2030 года с прогнозом на период до 2035 года» (2021). Получено из СПС «КонсультантПлюс»: https://www.consultant.

ru/document/cons_doc_LAW_402052/ (дата обращения: 16 октября 2025 г.).

24. Приказ Министерства транспорта Российской Федерации от 16 февраля 2011 г. № 56 «О Порядке информирования субъектами транспортной инфраструктуры и перевозчиками об угрозах совершения и о совершении актов незаконного вмешательства на объектах транспортной инфраструктуры и транспортных средствах» (2011). Получено из СПС «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_112010/ (дата обращения: 16 октября 2025 г.).
25. Винер, Н. (2019). *Cybernetics: or Control and Communication in the Animal and the Machine*. Cambridge; London: MIT Press. https://doi.org/10.7551/mitpress/11810.001.0001
26. Эшби, У. Р. (1954). *Design for a Brain: The Origin of Adaptive Behavior*. New York: Wiley. Получено с: https://ia801606.us.archive.org/32/items/designforbrainor00ashb/designforbrainor00ashb.pdf (дата обращения: 19 октября 2025 г.).
27. Месарович, М., & Такахара, Я. (1978). *Общая теория систем: математические основы*. Москва: Мир, 312 с. ISBN: 978-5-00000-000-0
28. Блауберг, И. В., & Юдин, Э. Г. (1973). *Становление и сущность системного подхода*. Москва: Наука, 270 с. EDN: https://elibrary.ru/RVCMPR
29. Садовский, В. Н. (1974). *Основания общей теории систем*. Москва: Наука, 280 с.
30. Богданов, А. А. (2020). *Тектология: всеобщая организационная наука*. Москва: Академический проект, 712 с. ISBN: 978-5-904954-54-3
31. Гройль, Г.-М., Лоссен, К., & Шустин, Е. (2007). *Introduction to Singularities and Deformations*. Berlin-Heidelberg: Springer, 471 с. ISBN: 978-3-540-28380-5
32. Соболев, С. Л., Китов, А. И., & Ляпунов, А. А. (2020). Основные черты кибернетики. В кн.: *Анатолий Иванович Китов* (с. 217–229). Москва: ООО «МАКС Пресс». EDN: https://elibrary.ru/RLEMIC

References

1. President of the Russian Federation. (2024). *Decree "On the Strategy for Scientific and Technological Development of the Russian Federation"*. Retrieved from the official legal information portal.
2. Ministry of Transport of the Russian Federation. (2025). *Report on the implementation of the Transport Strategy of the Russian Federation until 2030 with a forecast for the period up to 2035*. Retrieved from the official website of the Ministry of Transport of the Russian Federation.
3. International Civil Aviation Organization. (2019). *Aviation Benefits Report 2019*. Montreal: ICAO. Retrieved from: https://icao.assyst-uc.com/sites/default/files/sp-files/sustainability/Documents/AVIATION-BENEFITS-2019-web.pdf (Accessed: October 16, 2025)
4. International Transport Forum. (2023). *ITF Transport Outlook 2023*. Paris: OECD/ITF. https://doi.org/10.1787/b6cc9ad5-en
5. European Union Aviation Safety Agency. (2021). *Study on the societal acceptance of urban air mobility in Europe*. Cologne: EASA. Retrieved from: https://www.easa.europa.eu/sites/default/files/dfu/uam-full-report.pdf (Accessed: October 16, 2025)
6. Popov, E. A., Shtyrkhunova, N. A., & Abramyan, S. K. (2021). Evolution of transport security in Russia. *Humanities, Socio-Economic and Social Sciences*, *(4-2)*, 126–128. https://doi.org/10.23672/x7501-1481-8798-n. EDN: https://elibrary.ru/RGBUHA
7. Russian Federation. (2007). *Federal Law No. 16-FZ of February 9, 2007 "On transport security"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_66069/ (Accessed: October 16, 2025)
8. Federal Agency for Technical Regulation and Metrology. (2019). *GOST R 57119-2016. Methodology for assessing the vulnerability of transport infrastructure facilities and vehicles. General requirements*. Moscow: Standartinform, 18 p.
9. Federal Road Agency. (2014). *Order No. 2159-r of November 10, 2014 "On issuing and applying ODM 218.6.013-2014 'Methodological recommendations for developing transport security plans for transport*

infrastructure facilities and urban ground electric transport vehicles'". Retrieved from the official website of Rosavtodor: https://rosavtodor.gov.ru/docs/prikazy-rasporyazheniya/12717 (Accessed: October 16, 2025)

10. Federal Road Agency (Rosavtodor). (2011). *Order No. 871-r of November 15, 2011 "On issuing and applying ODM 218.4.007-2011 'Methodological recommendations for assessing the vulnerability of transport infrastructure facilities in the road sector' (together with 'ODM 218.4.007-2011. Sectoral road methodological document')"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_125293/ (Accessed: October 16, 2025)
11. Russian Railway Agency (Roszheldor). (2013). *Order No. 73 of March 7, 2013 "On revoking Order No. 515 of October 25, 2011 'On approving methodological recommendations for assessing the vulnerability of railway transport infrastructure and vehicles'"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_145508/ (Accessed: October 16, 2025)
12. International Civil Aviation Organization. (2024). *Global Aviation Security Plan*. Montreal: ICAO. Retrieved from: https://www.icao.int/sites/default/files/sp-files/Security/Documents/GLOBAL AVIATION SECURITY PLAN 2nd Ed.RU.pdf (Accessed: October 16, 2025)
13. International Civil Aviation Organization. (2017). *Aviation Security Manual (Doc 8973)* (10th ed.). Montreal: ICAO. ISBN: 978-92-9258-277-7
14. European Union Aviation Safety Agency. (2023). *Artificial Intelligence Roadmap 2.0: A human-centric approach to AI in aviation*. Cologne: EASA. Retrieved from: https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20 (Accessed: October 16, 2025)
15. Government of the Russian Federation. (2020). *Resolution No. 1605 of October 5, 2020 "On approving requirements for transport security, including anti-terrorism protection requirements for various categories of air transport infrastructure facilities"*. Retrieved from Consultant-

Plus: https://www.consultant.ru/document/cons_doc_LAW_364707/ (Accessed: October 16, 2025)

16. Government of the Russian Federation. (2020). *Resolution No. 1633 of October 8, 2020 "On approving requirements for transport security, including anti-terrorism protection requirements for various categories of railway transport infrastructure facilities"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_365316/ (Accessed: October 16, 2025)
17. Government of the Russian Federation. (2020). *Resolution No. 1637 of October 8, 2020 "On approving requirements for transport security for maritime and inland waterway transport vehicles"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_364993/ (Accessed: October 16, 2025)
18. Government of the Russian Federation. (2020). *Resolution No. 1638 of October 8, 2020 "On approving requirements for transport security, including anti-terrorism protection requirements for various categories of maritime and river transport infrastructure facilities"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_364994/ (Accessed: October 16, 2025)
19. Government of the Russian Federation. (2020). *Resolution No. 1640 of October 8, 2020 "On approving requirements for transport security for road and urban ground electric transport vehicles"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_364995/ (Accessed: October 16, 2025)
20. Government of the Russian Federation. (2020). *Resolution No. 1641 of October 8, 2020 "On approving requirements for transport security, including anti-terrorism protection requirements for various categories of off-street transport infrastructure facilities (in terms of metro systems)"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_365322/ (Accessed: October 16, 2025)
21. Government of the Russian Federation. (2020). *Resolution No. 1642 of October 8, 2020 "On approving requirements for transport security, including anti-terrorism protection requirements for various categories*

of road transport infrastructure facilities". Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_365313/ (Accessed: October 16, 2025)

22. Government of the Russian Federation. (2020). *Resolution No. 2201 of December 21, 2020 "On approving requirements for transport security, including anti-terrorism protection requirements for various categories of road infrastructure facilities"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_371982/ (Accessed: October 16, 2025)
23. Government of the Russian Federation. (2021). *Order No. 3363-r of November 27, 2021 "On the Transport Strategy of the Russian Federation until 2030 with a forecast for the period up to 2035"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_402052/ (Accessed: October 16, 2025)
24. Ministry of Transport of the Russian Federation. (2011). *Order No. 56 of February 16, 2011 "On the procedure for informing transport infrastructure operators and carriers about threats and acts of unlawful interference at transport infrastructure facilities and vehicles"*. Retrieved from ConsultantPlus: https://www.consultant.ru/document/cons_doc_LAW_112010/ (Accessed: October 16, 2025)
25. Wiener, N. (2019). *Cybernetics: Or control and communication in the animal and the machine*. Cambridge; London: MIT Press. https://doi.org/10.7551/mitpress/11810.001.0001
26. Ashby, W. R. (1954). *Design for a brain: The origin of adaptive behavior*. New York: Wiley. Retrieved from: https://ia801606.us.archive.org/32/items/designforbrainor00ashb/designforbrainor00ashb.pdf (Accessed: October 19, 2025)
27. Mesarovic, M., & Takahara, Y. (1978). *General systems theory: Mathematical foundations*. Moscow: Mir, 312 p. ISBN: 978-5-00000-000-0
28. Blauberg, I. V., & Yudin, E. G. (1973). *Formation and essence of the systems approach*. Moscow: Nauka, 270 p. EDN: https://elibrary.ru/RVCMPR
29. Sadovsky, V. N. (1974). *Foundations of general systems theory*. Moscow: Nauka, 280 p.

30. Bogdanov, A. A. (2020). *Tektology: General organizational science*. Moscow: Academic Project, 712 p. ISBN: 978-5-904954-54-3
31. Greuel, G.-M., Lossen, C., & Shustin, E. (2007). *Introduction to singularities and deformations*. Berlin Heidelberg: Springer, 471 p. ISBN: 978-3-540-28380-5
32. Sobolev, S. L., Kitov, A. I., & Lyapunov, A. A. (2020). Main features of cybernetics. In: *Anatoly Ivanovich Kitov* (pp. 217–229). Moscow: OOO "MAKS Press". EDN: https://elibrary.ru/RLEMIC

ДАННЫЕ ОБ АВТОРЕ

Ранверсман Алекс Евгеньевна, соискатель
Санкт-Петербургский государственный университет гражданской авиации имени Главного маршала авиации А. А. Новикова
ул. Пилотов, 38, г. Санкт-Петербург, 196210, Российская Федерация
a.ranversman@mail.ru

DATA ABOUT THE AUTHOR

Aleks E. Ranversman, degree seeking applicant
St. Petersburg State University of civil aviation named after Chief Marshal of aviation A. A. Novikov
38, Pilotov Str., St. Petersburg, 196210, Russian Federation
a.ranversman@mail.ru
SPIN-code: 1757-7020
ORCID: https://orcid.org/0009-0008-9363-2563

Поступила 22.10.2025
После рецензирования 10.11.2025
Принята 15.11.2025

Received 22.10.2025
Revised 10.11.2025
Accepted 15.11.2025