МЕЖОТРАСЛЕВОЙ СПЕЦИАЛИЗИРОВАННЫЙ ЖУРНАЛ

ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ И БЕЗОПАСНОСТЬ НА ТРАНСПОРТЕ

№ 16

ИЗДАЕТСЯ ПРИ ПОДДЕРЖКЕ ОБЩЕСТВЕННОГО СОВЕТА
ПРИ МИНИСТЕРСТВЕ ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

РАБОТА НА ОБЩИЙ РЕЗУЛЬТАТ



4







ТЕХНОЛОГИЧЕСКИЙ КОНТУР ТТК 10

ПРЕДИКТИВНАЯ БЕЗОПАСНОСТЬ 14

РОССИЯ НА НЕДЕЛЕ ИКАО 18

XIII НАЦИОНАЛЬНАЯ ПРЕМИЯ ЗА ДОСТИЖЕНИЯ В ОБЛАСТИ ТРАНСПОРТА И ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ



На главном отраслевом мероприятии «Транспортная неделя» состоится вручение XIII Национальной премии «Формула Движения».

В 2026 году премия присуждается в 8 номинациях:

— Лучший инфраструктурный проект;

— Лучший проект регионального значения;

— Лучшее инновационное решение в сфере транспортной техники;

— Лучшее решение в области цифровизации транспорта;

— Лучший проект в области беспилотных технологий на транспорте;

— Лучшее решение в сфере обеспечения транспортной безопасности;

— Лучший проект в интересах семьи;

— Лучший работник транспорта России.

Премия была учреждена в 2014 году Общественным советом при Министерстве транспорта Российской Федерации и призвана содействовать развитию транспортной инфраструктуры, повышению уровня транспортных услуг, а также стимулированию государственных и коммерческих структур к решению значимых проблем транспортной сферы России. Вручение XIII Национальной премии «Формула Движения» по традиции станет частью главного отраслевого мероприятия «Транспортная неделя», которое пройдет с 14 по 20 ноября в Москве.

В рамках «Транспортной недели» с 18 по 20 ноября в Гостином Дворе состоятся XX Международный форум и выставка «Транспорт России». В деловую программу «Транспорта России» прошлого года вошло свыше 40 мероприятий (сессии, конференции, дискуссии, круглые столы и презентации), где выступили около 400 спикеров. На выставке свои разработки продемонстрировали более 120 компаний транспортного сектора. Участниками деловой программы стали свыше 5 тыс. человек, выставку посетило более 12 тыс. человек.





16+

Фото: 2025.transweek.digital



Вячеслав Керов,
главный редактор журнала, председатель Комиссии по вопросам транспортной безопасности и безопасности на транспорте Общественного совета при Министерстве транспорта Российской Федерации

Уважаемые коллеги!

Главная тема и центральный материал этого номера – назначение Указом Президента РФ от 22.10.2026 № 769 на должность Министра транспорта Российской Федерации Дмитрия Викторовича Ядрова и представление его коллективу министерства заместителем Председателя Правительства Российской Федерации Андреем Сергеевичем Никитиным. Он отметил, что кандидатура нового Министра транспорта получила единогласную поддержку Президента, Правительства и Государственной Думы, а также подчеркнул профессиональные и управленческие качества Дмитрия Викторовича Ядрова. Об этом в начале номера большой фоторепортаж.

Заместитель Министра транспорта Российской Федерации Евгений Станиславович Филиппов в эксклюзивном интервью нашему журналу рассказал о главной особенности современной системы безопасности на транспорте, о том, как работает подсистема мониторинга ЧС на транспорте, о переходе к предиктивной модели, то есть о смещении акцента с ретроспективной аналитики рисков на проактивное прогнозирование.

Особого внимания заслуживает публикация выступления первого заместителя Министра транспорта Российской Федерации Константина Анатольевича Пашкова на пленарной сессии «Стратегические направления технологического развития Трансарктического транспортного коридора для освоения Арктики» 7-й Международной выставки и конференции по судостроению и разработке высокотехнологичного оборудования для освоения Арктики и континентального шельфа.

Выход этого номера приурочен к юбилейному XX Международному форуму и выставке «Транспорт России», где журнал будет широко представлен на стендах, сессиях и отраслевых конференциях Минтранса России, Общественного совета при Минтрансе России, Федеральной службы по надзору в сфере транспорта и других отраслевых организаций. В рамках Форума состоится вручение XIII Национальной премии за достижения в области транспорта и транспортной инфраструктуры «Формула Движения», в том числе в номинации «Лучшее решение в сфере обеспечения транспортной безопасности». Следующий номер журнала широко осветит вопросы по транспортной безопасности, поднятые на мероприятиях «Транспортной недели».

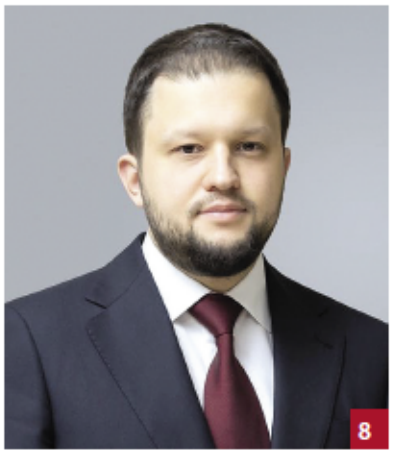
Все больше материалов журнала посвящено информационной безопасности, которая сейчас является неотделимой частью транспортной безопасности. Так, в этом номере подробно рассказывается о недавно прошедшей научно-практической конференции «Авиакод: новые стандарты и передовые ИБ-решения для авиации», которая собрала около 230 представителей авиационной отрасли.

Темы транспортной (авиационной) безопасности и информационной безопасности вновь станут основной повесткой дня на Всероссийской конференции «Транспортная безопасность: защита объектов воздушного транспорта», которая пройдет 3 декабря 2026 года во Внуково. Деловая программа конференции начнется с открытого заседания Комиссии по вопросам транспортной безопасности и безопасности на транспорте Общественного совета при Министерстве транспорта Российской Федерации. На конференции будут подняты вопросы повышения эффективности защиты объектов транспортной инфраструктуры воздушного транспорта от актов незаконного вмешательства и киберугроз.

До встречи на «Транспортной неделе 2026» и других отраслевых мероприятиях!

КОМИССИЯ ОБЩЕСТВЕННОГО СОВЕТА ПРИ МИНИСТЕРСТВЕ ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Содержание











Работа на общий результат 4

Российским авиакомпаниям – отечественные самолеты 8

Технологический контур ТТК: флот, наука, кадры 10

Предиктивная безопасность 14

Неделя ИКАО по авиационной безопасности 18

Новые инициативы и тиражируемые решения 22

Минтранс и ФТС: основы продуктивного взаимодействия 24

От данных – к решениям 28

Категорирование объектов КИИ воздушного транспорта 32

«Авиакод 2026» и цифровая устойчивость гражданской авиации 34

Защита объектов критической информационной инфраструктуры в авиации 36

Функциональная устойчивость транспорта: как сохранить перевозки при цифровых сбоях 46

Тренды кибербезопасности – 2027: к чему готовиться транспортной отрасли 48

Цифровизация транспорта: систем больше, а управления меньше? 50

На III Всероссийском форуме «Транспортная реформа» обсудили будущее отрасли 52





«Студенческий» аэропорт: как молодость влияет на транспортную безопасность 54

Ответственность следует за грузом 58

Противодействие БПЛА в сфере транспортной безопасности – от оценки уязвимости до пресечения деятельности: нормативное регулирование и проблемные вопросы 60

Противодействие новым угрозам для объектов транспортной инфраструктуры 62

Постановление № 588: правовой фундамент создан – нужна инженерная опора 64

ТСНК закрывает контейнерную брешь в системе транспортной безопасности 66

Радиологический терроризм: тонкая грань между пациентом и террористом 68

Радиосвязь в аэропортах: устойчивость, безопасность и независимость инфраструктуры 70

Границы автоматического досмотра 72

Комплексное оснащение пунктов досмотра на объектах транспортной инфраструктуры: критерии выбора и взаимодействие технических средств 74

Аппаратура радиационного контроля для ОТИ 76



ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ И БЕЗОПАСНОСТЬ НА ТРАНСПОРТЕ

№ 16 (2026 г.)
Издается с 2022 года

Регистрационный номер СМИ: ПИ № ФС77-84141 от 09.11.2022 г. СМИ зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Учредитель: ООО «ЦУМПП»

Периодичность выхода: 4 выпуска в год

Тираж: 4000 экз.

Распространение: целевые рассылка и распространение

Территория распространения: Москва и регионы Российской Федерации

Фото на обложке: пресс-служба Минтранса России, Ространснадзор

Главный редактор: Керов Вячеслав Всеволодович

Заместитель главного редактора: Никитушин А. С.

Советник главного редактора: Лоран Б. О.

Шеф-редактор: Шитикова Е. М.

Продвижение журнала в соцсетях: Лоран Д. Б., Лоран О. Б.

Дизайн и верстка: Войлокова Н. В.

Корректор: Балашова Е. А.

Адрес учредителя: 125480, г. Москва, ул. Героев-Панфиловцев, д. 24, оф. 208, тел.: + 7 (925) 575-85-71; e-mail: info@tsumpp.ru

Адрес редакции: 119415, г. Москва, просп. Вернадского, д. 39, оф. 613, тел.: +7 (495) 784-17-92; e-mail: vkerov@osmintrans.ru

Реклама и распространение: ООО «ЦУМПП»

Мнение редакции не всегда может совпадать с мнением авторов. За точность и достоверность изложенной информации отвечают авторы. За содержание рекламных материалов редакция ответственности не несет.

Дата выхода в свет: 16.11.2026 г.
Отпечатано в типографии ОАО «Подольская фабрика офсетной печати», 142100, г. Подольск, Революционный проспект, д. 80/42.
Номер заказа
Распространяется бесплатно.

РАБОТА НА ОБЩИЙ РЕЗУЛЬТАТ



Заместитель Председателя Правительства Российской Федерации Андрей Никитин представил Министра транспорта Российской Федерации Дмитрия Ядрова коллективу министерства. Дмитрий Ядров был назначен на эту должность Указом Президента РФ от 22.10.2026 № 769.

Глава Минтранса России имеет уникальный опыт работы в отрасли – более 16 лет. Дмитрий Ядров девять лет трудился в Госкорпорации по организации воздушного движения, пройдя путь от диспетчера радиолокационного управления и процедурного контроля до директора по стратегическому развитию корпорации. С 2019 по 2026 год работал в подведомственном Минтрансу Федеральном агентстве воздушного транспорта, сначала в должности заместителя, затем – руководителем агентства.

Андрей Никитин отметил, что кандидатура нового Министра транспорта получила единогласную поддержку Президента, Правительства и Государственной Думы, а также подчеркнул его профессиональные и управленческие качества.

«Мы знаем Дмитрия Викторовича как человека системного, умеющего принимать решения и доводить начатое до конца. В то же время он умеет слушать и слышать позицию, балансировать эту позицию, – подчеркнул вице-премьер. – Транспорт сегодня – это отрасль, которая в наибольшей степени обладает системным подходом и управленческой вертикалью. И особая ценность нашей с вами работы – то, что транспортники присутствуют на самых разных уровнях власти. И не существует отдельного результата у зампреда Правительства, у Правительства, у Министра, у глав федеральных агентств, у Государственной Думы. Есть единый результат – это надежность и эффективность транспортной системы, и каждый на своем месте будет добиваться этого результата».



Андрей Никитин



Андрей Никитин и Дмитрий Ядров









Дмитрий Ядров

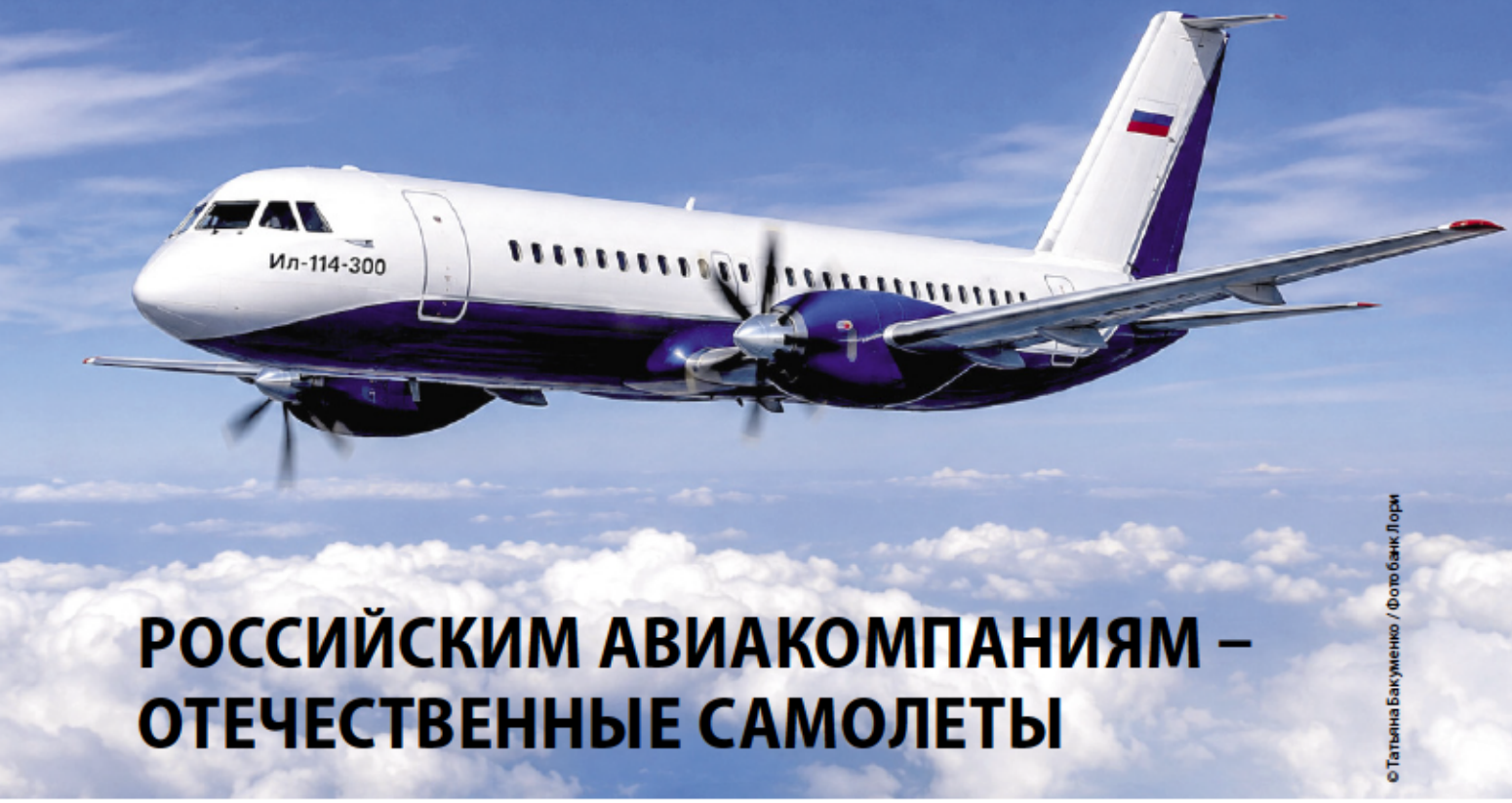
Дмитрий Ядров поблагодарил коллектив Росавиации, с которым он работал долгие годы, и отметил, что в Минтрансе сформирована сильная команда, с которой он намерен продолжить выполнять все задачи, поставленные перед транспортным комплексом руководством страны.

«Задачи, которые сегодня стоят перед нами, требуют максимальной отдачи, четкой координации усилий и взвешенных решений, – сказал глава Минтранса. – Наш главный приоритет – это эффективная реализация ключевых задач, поставленных Президентом России Владимиром Путиным, и обеспечение позитивных результатов для граждан. Уверен, что, опираясь на профессионализм вверенного мне коллектива, мы сможем реализовать все национальные проекты».

За большой личный вклад в проведение государственной политики в области транспорта Дмитрий Ядров вручил Андрею Никитину знак отличия Министра транспорта Российской Федерации «За труд и пользу».

По материалам Минтранса России





© Татьяна Бакуменко / Фотобанк Лори

РОССИЙСКИМ АВИАКОМПАНИЯМ – ОТЕЧЕСТВЕННЫЕ САМОЛЕТЫ

22 октября Президент Российской Федерации Владимир Путин подписал указ о назначении руководителя Росавиации Дмитрия Ядрова Министром транспорта Российской Федерации. В этот день состоялось заседание Общественного совета при Росавиации, одной из тем которого стало обеспечение российских авиакомпаний отечественными воздушными судами.



Дмитрий Ядров,
Министр транспорта Российской Федерации

«Реализация указа Президента России о национальных целях до 2030 года и перспективу до 2036 года в части обеспечения российских авиакомпаний отечественными воздушными судами – важнейшая тема для всей авиационной отрасли. Сложности, возникающие в ходе импортозамещения, – один из текущих сдерживающих факторов роста авиационных перевозок. При обсуждении данного вопроса мы регулярно сталкиваемся с критикой, но работа в этом направлении ведется очень плотно. Отмечу, что вопрос находится на контроле Правительственной комиссии по промышленности, которую возглавляет первый заместитель Председателя Правительства РФ Денис Мантуров.

Действительно, уже очень многое сделано. Получены первые сертификаты типа, в частности на российские импортозамещенные пассажирские самолеты Ту-214, Ил-114-300 и двигатель ПД-8. В ближайшее время будет завершена работа по импортозамещенным версиям самолетов «Суперджет 100» и МС-21.

Близится к завершению сертификация двигателя и воздушного винта для нового легкого самолета «Байкал». Надеюсь, что промышленность оперативно предоставит все доказательные документы в Росавиацию. И в конце этого года или в начале следующего работа по двигателю закончится, будет выдан сертификат и на двигатель, и на винт. Задержка с реализацией проекта самолета «Байкал» связана с зарубежными санкциями, из-за которых потребовалось заменить импортный двигатель отечественным.

Российско-белорусский самолет «Освей» вместимостью 19 пассажиров планируется сертифицировать в 2029 году. Эти машины будут сильно востребованы – спрос со стороны авиакомпаний есть уже сейчас.

Можно долго обсуждать, почему все это произошло, вспоминать о том, как было в Советском Союзе, но нужно понимать, что мы – вторые в мире после СССР, кто производит свои магистральные и региональные самолеты без международной кооперации, по нормам и требованиям, которые полностью коррелируются с современными международными стандартами. В те сроки, которая наша промышленность реализует проекты по созданию импортозамещенных версий (фактически это создание самолетов с нуля), не укладывалась ни одна страна.

Коллеги, на протяжении трех лет (Дмитрий Ядров возглавил Росавиацию в сентябре 2023 года. – ***Прим. ред.***) мы с вами усердно трудились и многого добились: это касается и кадров, и аэродромов, и сертификации авиационной техники, и внутренней работы Росавиации и работы с Общественным советом. Эту работу, безусловно, продолжу и буду делать все, чтобы наша гражданская авиация была устойчивой, безопасной и функционировала стабильно.

Мы – одна команда. Все результаты, о которых я говорил, оказались достигнутыми только благодаря совместной плодотворной работе. В нашей отрасли есть очень много сложных задач, и нужно находить пути их решения. Мы всегда их находили и, уверен, найдем и в этот раз и завершим все текущие проекты, продолжая работать единой командой». ■

Фото: пресс-служба Росавиации, фотобанк Лори



© Виктор Карасев / Фотобанк Лори

ТЕХНОЛОГИЧЕСКИЙ КОНТУР ТТК: ФЛОТ, НАУКА, КАДРЫ

Выступление на пленарной сессии «Стратегические направления технологического развития Трансарктического транспортного коридора для освоения Арктики» 7-й Международной выставки и конференции по судостроению и разработке высокотехнологичного оборудования для освоения Арктики и континентального шельфа (OMR 2026). Санкт-Петербург. Мариинский дворец. *9 октября 2026 года.*



Константин Пашков,
первый заместитель Министра транспорта Российской Федерации

ЧТО СДЕЛАНО ЗА ГОД

Как сказал Президент России Владимир Путин, «скорость технологических изменений нарастает стремительно, идет резко вверх – тот, кто использует эту технологическую волну, вырвется далеко вперед». В Арктике каждый месяц реализуются решения, который меняют всю транспортную отрасль, в том числе нашу работу в Арктике.

Северный морской путь (СМП) заметно перешел от отдельных проектов к формированию устойчивой транспортной системы. Это видно одновременно по развитию флота, росту международных перевозок и созданию инфраструктуры мониторинга. Главное изменение – расширение международного измерения Трансарктического транспортного коридора (ТТК).

В октябре 2025 года Россия и Китай договорились о развитии перевозок по СМП с перспективой увеличения объемов до 20 млн тонн. Первый иностранный контейнерный экспресс Istanbul Bridge совершил транзитный рейс из Китая в Европу (Великобританию) через Арктику.

В ноябре 2025 года на Балтийском судостроительном заводе при участии Президента России Владимира Путина состоялась закладка атомного ледокола «Сталинград».

В декабре 2025 года в эксплуатацию введен первый российский арктический газовоз «Алексей Косыгин». Концентрация атомных ледоколов на СМП стала рекордной – одновременно восемь единиц.

В январе текущего года подведены итоги грузовых перевозок по СМП за 2025 год – 37 млн тонн.

В феврале три ледокола обеспечивали проводку судов к порту Эльга.

В апреле на Международном транспортно-логистическом форуме с представителями 82 государств обсуждалась новая модель ТТК.

В мае завершено формирование космического комплекса мониторинга СМП. В состав средств наблюдения входят: «Арктика-М» – гидрометеорологический спутник для мониторинга Арктики; «Кондор-ФКА» – радиолокационный спутник дистанционного зондирования Земли; «Метеор-М» – метеорологический спутник для наблюдения за Землей.

В июне в эксплуатацию введен второй российский арктический газовоз «Константин Посьет».

В августе китайская компания «СиалЭйджен Шипинг» приступила к регулярным контейнерным перевозкам по арктическому маршруту.

В сентябре южнокорейская компания «Панстар Лайн» выполнила первый экспериментальный контейнерный рейс по арктическому маршруту.

В октябре проведена международная конференция OMR 2026.

В декабре ожидается завершение строительства аварийно-спасательного судна «Керченский пролив», которым занимается Амурский судостроительный завод.

СЕВЕРНЫЙ МОРСКОЙ ПУТЬ – ТРАНСПОРТНЫЙ КОРИДОР

Наши партнеры и конкуренты не дремлют. Китай уже использует ИИ для 15-дневного прогноза



ледовой обстановки. Норвегия развивает спутниковое наблюдение за движением судов, Дания – беспилотные системы длительного патрулирования, Канада – загоризонтные радиолокационные комплексы. США и Финляндия наращивают ледокольные возможности. То есть сегодня конкуренция в Арктике идет уже не только за маршруты, но за контроль с помощью технологий. Для нас технологическим ответом должно стать усиление собственных конкурентных преимуществ.

Именно поэтому Президент поставил задачу смотреть на СМП шире – как на ключевой участок ТТК. Это не только морская трасса. В него встроены морские порты и речные пути, железные дороги, подходы к портам, связь, навигация, спутниковые технологии, спасательная инфраструктура и цифровые сервисы.

Развитие Большого Северного морского пути входит в состав национального проекта «Эффективная транспортная система». Затраты из бюджета на его реализацию до 2030 года составляют 253,2 млрд рублей.

Нам предстоит прокладывать не только надежные, но и безопасные морские маршруты в Арктике и выходить на круглогодичную работу ТТК.

Чтобы работа ледоколов и танкеров была стабильной, Минтранс развивает аварийно-спасательный флот. В акватории СМП сейчас задействовано 14 судов.



К 2030 году пополним аварийно-спасательный флот еще 10 судами. Учитывая сложность задачи, Минтранс (Росморречфлот) выступил заказчиком судов с уникальными характеристиками.

ВКЛАД ТРАНСПОРТНОЙ НАУКИ В РЕШЕНИЕ НАУЧНЫХ ЗАДАЧ В АРКТИКЕ

Сегодня в 11 научных и 28 научно-образовательных организациях Минтранса России ведутся исследования по 8 направлениям, связанным с работой транспорта на СМП.

Среди них:

- гидрографическое и гидрометеорологическое обеспечение безопасного судоходства;
- моделирование и оптимизация маршрутов СМП;
- повышение эффективности организации транспортных потоков;
- оценка рисков и уровня аварийно-спасательной готовности флота;
- влияние судоходства на экосистему Арктики;
- автономное судоходство в Арктической зоне;
- гидрографическое обеспечение функционирования портовой инфраструктуры;
- интеграция железных дорог в инфраструктуру портовой системы СМП.

Но научных задач, относящихся к вопросам развития перевозок по СМП, гораздо больше. Традиционно мы активно работаем с РАН по этим вопросам. Тема развития транспортных систем в Арктике заложена в Концепции научно-технологического развития транспортного комплекса Российской Федерации на период до 2035 года.

ПЕРЕДОВАЯ ИНЖЕНЕРНАЯ ШКОЛА «АРКТИКА»

Сегодня вся Арктическая зона дает около 6% ВВП России и около 10% экспорта. Мультипликатор наших инвестиций в Арктику для машиностроения, нефте- и газодобычи, промышленного и градского строительства – еще больше. Вклад в экономический суверенитет и благополучие людей неизмерим деньгами.

Говоря о научной составляющей, отмечу, что нам нужна не просто новая образовательная программа. Нужна передовая инженерная школа обеспечения безопасности морского судоходства в сложных ледовых условиях, с малой гидрографической изученностью, энергообеспечения строительства и функционирования крупных инфраструктурных объектов Арктической зоны.

Нам нужен стартап, который будет проектировать и создавать технологии и методологию проводки судов ледового класса и ледоколов на трассах СМП, а также безопасного и эффективного функционирования объектов энергогенерации для следующего поколения арктического мореплавания, и одновременно готовить людей, способных эти технологии создавать и грамотно эксплуатировать.

С 1958 года подготовка специалистов по эксплуатации гражданских судов с ядерными энергетическими установками проводится в единственном в своем роде учебном заведении нашей страны – в Макаровке.





Здесь есть кадры, лаборатории, тренажеры. Таким образом, в стране уже 70 лет формируется уникальный центр компетенций – морских, ледовых и ядерных.

Предлагается создать Передовую инженерную школу именно здесь, в Санкт-Петербурге, на базе Государственного университета морского и речного флота имени адмирала С. О. Макарова.

Задача школы – сформировать полный образовательный и технологический/инженерный контур ТТК: «судно – порт – энергетика – данные – управление». С точки зрения энергетики драйвером развития могут стать модернизированные плавучие энергоблоки (МПЭБы), с точки зрения обеспечения безопасного мореплавания – ледоколы, включая самый мощный в мире атомный ледокол типа «Лидер».

Арктическое мореплавание требует отдельной инженерной школы, потому что здесь соединяются сразу несколько сложнейших задач. Судно должно работать во льдах и экстремальном климате, получать данные с воздуха и из-под воды, взаимодействовать с береговой инфраструктурой, обеспечивать безопасность и экологический контроль.

Партнерами ПИШ могут выступить Госкорпорация «Росатом», ФГУП «Атомфлот», Научно-исследовательский технологический институт имени А. П. Александрова, Опытно-конструкторское бюро машиностроения имени И. И. Африкантова.

Уверен, эта идея найдет поддержку у присутствующих здесь коллег.

ИНФРАСТРУКТУРА СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

В завершение хочу отметить несколько фактов. История российского транспорта показывает: самые смелые проекты становятся инфраструктурой следующего поколения.

140 лет назад открытие Ново-Мариинского канала (при министре путей сообщения К. Н. Посьете) связывало отдельные водные бассейны в единую систему.

110 лет назад железная дорога дошла до незамерзающего Мурманского побережья – Россия создавала новый круглогодичный выход к морю.

Сегодня перед нами задача того же масштаба – связать в единую систему СМП, порты, железные дороги, реки, флот, космическую инфраструктуру и цифровые сервисы. Тогда ТТК станет не просто направлением движения грузов, а полноценной международной транспортной системой.

А значит, как и сто и более лет назад, успех будет определяться тем, сумеем ли мы заранее создать необходимые технологии, подготовить инженеров и построить инфраструктуру для следующего витка развития страны.

Замечу, что вопросам арктического мореплавания всегда уделяется особое внимание у нас в Министерстве, в Правительстве, в транспортном комплексе в целом, в деловом и академическом сообществе. ■

Иллюстрации: пресс-служба Минтранса России

ПРЕДИКТИВНАЯ БЕЗОПАСНОСТЬ

Заместитель Министра транспорта Российской Федерации Евгений Филиппов – о том, как работает подсистема мониторинга ЧС на транспорте.



Евгений Филиппов,
заместитель Министра транспорта Российской Федерации

– Евгений Станиславович, в чем главная особенность современной системы безопасности на транспорте?

– Масштаб транспортной сети нашей страны – это сотни тысяч объектов, и в такой сложной инфраструктуре вероятность нештатных ситуаций всегда на особом контроле. Главная особенность нашей работы в том, что мы уходим от простой фиксации происшествий к предиктивной безопасности – то есть к прогнозированию угроз до того, как они станут реальными ЧС.

Для этого действует функциональная подсистема мониторинга и информирования о чрезвычайных ситуациях на объектах транспортной инфраструктуры. Это часть единой государственной системы предупреждения и ликвидации ЧС (РСЧС), но созданная специально для транспортного комплекса.

В прошлом году в перечень сил и средств постоянной готовности федерального уровня Министерства транспорта был включен СИЦ Минтранса России – и именно на его базе сформирована седьмая функциональная подсистема, отвечающая за мониторинг и информирование о ЧС на транспортных объектах.

– На какой правовой и организационной основе все это работает?

– Безопасность на транспорте – это вопрос жизни и здоровья миллионов людей и устойчивости всей экономики. Государство регулирует эту сферу при помощи федерального закона о защите от чрезвычайных ситуаций (Федеральный закон №68-ФЗ), а также посредством единой государственной системы предупреждения и ликвидации ЧС (РСЧС). Она похожа на многоуровневую сеть и представлена на каждом уровне – от федерального до муниципального.

Транспорт – особая зона риска: аварии, наводнения, пожары могут парализовать целые регионы. Поэтому у Минтранса России есть собственная сеть – функциональные подсистемы, которые создаются ведомствами для своих отраслей.

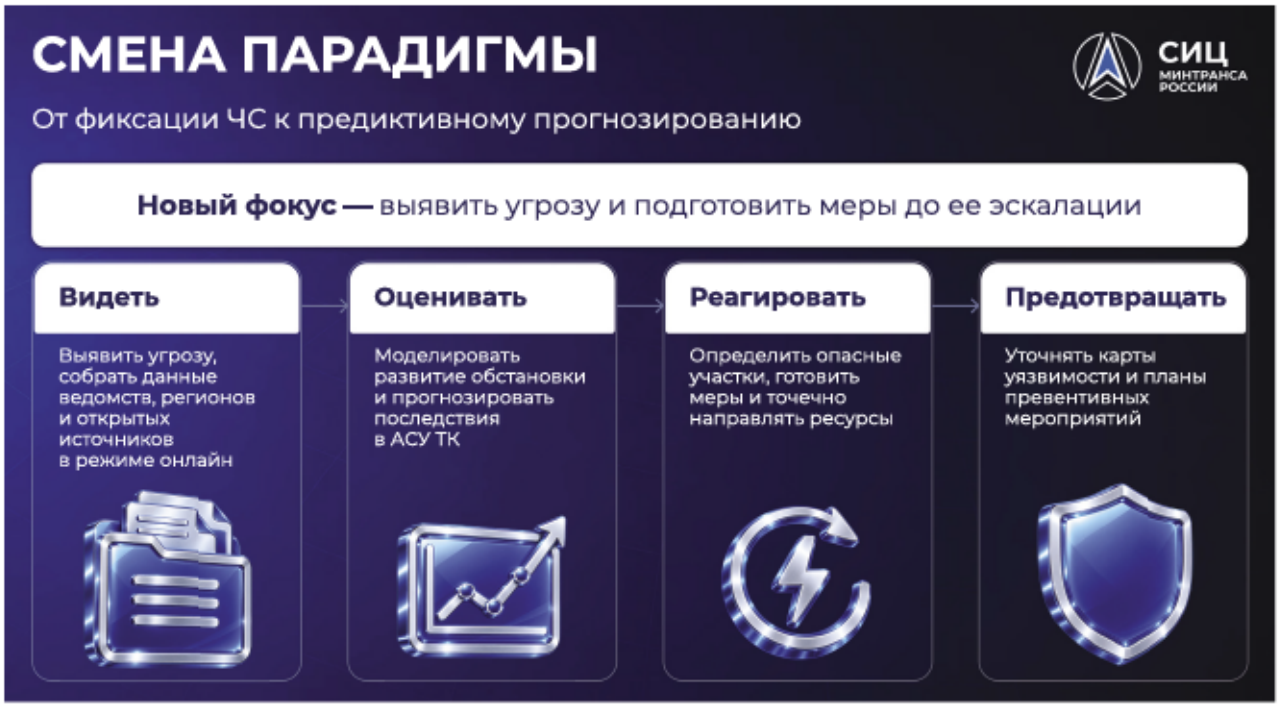
– Вы упомянули переход к предиктивной модели. Что конкретно это значит на практике?

– Это значит смещение акцента с ретроспективной аналитики рисков на проактивное прогнозирование. Раньше мы, в основном, анализировали, что уже случилось, и делали выводы. Сейчас задача – заранее видеть угрозы, просчитывать сценарии и готовить меры реагирования до эскалации.

Подсистема собирает данные о ЧС и угрозах из множества источников: от подведомственных служб Минтранса, других ведомств, регионов, а также из открытых источников. Это дает максимально полную картину обстановки в режиме онлайн. Дальше идет этап оценки рисков с помощью специальных аналитических инструментов, в первую очередь – Автоматизированной системы управления транспортным комплексом (АСУ ТК). Она помогает моделировать развитие ситуации и прогнозировать последствия. Такой подход позволяет заблаговременно определять потенциально опасные участки и точечно направлять ресурсы.

– Как конкретно это работает на практике?

– Цели подсистемы можно сформулировать как «видеть, оценивать, реагировать, предотвращать». Данные, которые в ней собираются, используются не только для оперативных сводок, но и для долгосрочного



прогнозирования. На их основе мы уточняем карты уязвимых участков инфраструктуры, корректируем планы превентивных мероприятий, совершенствуем алгоритмы межведомственного взаимодействия.

В итоге это не просто инструмент реагирования, а полноценная система управления рисками. И экономическая составляющая здесь тоже важна: чем раньше выявлен риск, тем меньше сил и средств уходит на его нейтрализацию. Снижается нагрузка на бюджет, уменьшаются потери от сбоев в грузо- и пассажиропотоках – а высвобожденные ресурсы можно направить на развитие инфраструктуры. Но главное, конечно, – безопасность пассажиров: своевременное предупреждение позволяет предотвращать трагедии и спасать жизни.

– Отдельно хотелось бы поговорить про АСУ ТК. Как система в целом помогает укреплять безопасность транспортного комплекса?

– АСУ ТК – это ядро информационно-аналитической платформы регулирования на транспорте. Ее задача – формировать единую цифровую картину транспортного комплекса в режиме реального времени. Для этого система интегрирует данные из разных источников: от ведомственных служб, метеослужб, систем мониторинга природных явлений, а также от подведомственных агентств и открытых источников.

АСУ ТК решает сразу несколько задач. Во-первых, она создает единое информационное пространство для Минтранса и смежных ведомств – например, МЧС, Росгидромета и других, – чтобы координация была быстрее и точнее. Во-вторых, система автоматизирует сбор и обработку показателей: речь идет о десятках тысяч метрик, характеризующих состояние инфраструктуры, транспортных потоков и нештатных ситуаций. В-третьих, АСУ ТК поддерживает инструменты предиктивной аналитики: модели оценки развития обстановки, сценарное моделирование, расчет последствий, о чем мы уже говорили ранее. Все это позволяет принимать управленческие решения на основе данных, в том числе в вопросах безопасности.

И, конечно, это часть большой цифровой трансформации: АСУ ТК становится «нервной системой» отрасли, связывая между собой разные виды транспорта, ведомства и уровни управления. Именно такая интеграция позволяет добиваться не точечных улучшений, а системного эффекта – более безопасных, надежных и экономически эффективных перевозок.

– В чем состоит роль АСУ ТК как связующего звена между оперативным реагированием и долгосрочным планированием в сфере транспортной безопасности?

– АСУ ТК выступает тем самым мостом, который превращает оперативные данные в стратегические решения. На уровне оперативного реагирования система в реальном времени фиксирует отклонения (например, рост аварийности на участке) и сразу подсвечивает риски ответственным службам. Одновременно эти же данные накапливаются и становятся базой для долгосрочного планирования: на их основе мы формируем карты уязвимости, пересматриваем приоритеты



ремонта, корректируем маршруты объездов и обновляем регламенты взаимодействия ведомств.

Например, если на каком-то участке из-за подтоплений трижды за сезон приходилось перекрывать движение, АСУ ТК не просто фиксирует эти инциденты: она анализирует их, связывает с историей ремонтов и нагрузкой на дорогу, чтобы обосновать необходимость строительства водоотвода или переноса трассы. То есть система не только помогает избежать ЧП здесь и сейчас, но и системно снижает риски в будущем – за счет того, что каждое оперативное событие становится аргументом для долгосрочных изменений. Это и есть ее системная роль: обеспечивать преемственность между тактикой и стратегией в управлении безопасностью транспортного комплекса. ■

Беседовал Вячеслав Керов

Иллюстрации: пресс-служба Минтранса России



«Транспортная неделя – 2026» – главное деловое событие транспортной отрасли России

Даты проведения: 14–20 ноября 2026 года

Ключевое событие: XX Международный форум и выставка «Транспорт России» пройдут с 18 по 20 ноября в московском Гостином Дворе

Организатор: Министерство транспорта Российской Федерации (по распоряжению Правительства Российской Федерации)

Главная тема: «Транспортная стратегия России до 2050 года»

В фокусе внимания – формирование единой транспортной системы с учетом развития экономики, укрепления суверенитета и технологических изменений. Участники обсудят повышение мобильности граждан, развитие цифровой логистики, внедрение искусственного интеллекта, технологическую независимость и другие ключевые ориентиры транспортного комплекса на перспективу до 2050 года. В повестку форума также войдут вопросы развития беспилотных перевозок, цифровизации и платформенных решений, транспортной инфраструктуры и логистики, привлечения инвестиций и другие актуальные направления отрасли.





В рамках деловой программы запланировано более 30 форматов – сессии, конференции, круглые столы. В центре внимания выставки «Транспорт России» будет объединенный стенд национальных проектов и экспозиции компаний-участников выставки.

Фото: 2025.transweek.digital



НЕДЕЛЯ ИКАО ПО АВИАЦИОННОЙ БЕЗОПАСНОСТИ

В столице Республики Казахстан Астане с 20 по 22 октября прошла Неделя авиационной безопасности (ICAO Security Week 2026), проведенная Международной организацией гражданской авиации (ИКАО) и авиационными властями Казахстана.



Владимир Черток,
советник руководителя Федеральной службы по надзору в сфере транспорта, действительный государственный советник Российской Федерации, национальный координатор по авиационной безопасности в системе Универсальной программы проверок авиационной безопасности в государствах с учетом механизма непрерывного мониторинга и официальный эксперт по авиационной безопасности Международной организации гражданской авиации (ИКАО)

Широкое представительство делегаций из 62 государств-членов ИКАО и более 1000 участников девяти основных и целого ряда параллельных сессий Недели обеспечили возможность всестороннего обсуждения новых угроз и рисков, а также быстрого роста некоторых известных типовых угроз с целью выработки практических подходов к обеспечению авиационной безопасности в условиях современных и будущих вызовов.

В соответствии с решением Минтранса и МИД России делегацию Российской Федерации на Неделе возглавил руководитель Федеральной службы по надзору в сфере транспорта **Виктор Гулин**, а в ее состав вошли представители департаментов Минтранса и МИД России, Представительства Российской Федерации при ИКАО, Ространснадзора, ГосНИИ ГА, авиакомпании «Россия», аэропорта Домодедово, учебных центров по авиационной и транспортной безопасности, предприятий-изготовителей технических средств транспортной безопасности.

Началу Недели в Астане предшествовали заседания Рабочей (экспертной) группы по авиационной безопасности при Совете руководителей уполномоченных органов в области транспорта государств-членов Евразийского экономического союза и Координационной группы по авиационной безопасности стран Центральной Азии и Кавказа, на которых были рассмотрены наиболее актуальные вопросы взаимодействия и общие подходы к предстоящим обсуждениям на сессиях Недели.

На открытии Недели под девизом «Безопасное небо в сложном мире: повышение авиационной безопасности для всех» участники выслушали приветственные обращения Министра транспорта Республики Казахстан **Нурлана Сауранбаева** и Генерального секретаря ИКАО **Хуана Карлоса Саласара**.

На пленарном заседании высокого уровня руководитель Ространснадзора – руководитель делегации Российской Федерации выступил с докладом об инновациях в национальном государственном надзоре за обеспечением авиационной безопасности и авиационной кибербезопасности и развитию международного и регионального сотрудничества в этой сфере. Также выступили представители Канады, Африканской и Латиноамериканской комиссий гражданской авиации.

На **сессии № 1 «25 лет спустя: глобальное состояние безопасности в авиации»** по предложению руководства ИКАО в качестве спикера выступил советник руководителя Ространснадзора, официальный эксперт ИКАО по авиационной безопасности **Владимир Черток,** спикерами сессии были также представители США, Казахстана и Уганды.

В ходе обсуждения было отмечено, что Стандарты и Рекомендуемая практика ИКАО доказали свою эффективность, однако ландшафт новых

угроз и рисков быстро меняется, порождая и новые уязвимости в системах безопасности. Центральная тема дискуссии – способность государств и всей авиационной отрасли перейти от реагирования на фактические угрозы к их упреждению на основе прогнозирования, анализа рисков и взаимодействия государств и индустрии.

Сессия № 2 «Замыкая цикл: от результатов аудитов к устойчивому потенциалу» слушала выступления спикеров из Эфиопии, Таиланда, Казахстана и Исполнительного директората Контртеррористического комитета ООН, посвященные ценности аудитов комиссиями ИКАО по Универсальной программе проверок авиационной безопасности с использованием механизма непрерывного мониторинга. Их практическая эффективность измеряется не отчетами, а корректирующими действиями, согласованными государством и ИКАО, устраняющими коренные причины несоответствий международным стандартам и формирующими долгосрочный устойчивый потенциал безопасности.

Отмечено, что корректирующие действия по итогам аудитов ИКАО по авиационной безопасности и авиационной кибербезопасности следует рассматривать как дорожную карту инвестиций в национальную безопасность государств. Показана неразрывная связь позитивных результатов аудитов ИКАО и эффективности национальных государственных систем надзора за обеспечением авиационной безопасности.

Сессия № 3 «Соответствует ли замыслу? Глобальный план авиационной безопасности и путь к достижению целевого ориентира» заслушала спикеров из Кении, Латвии, Африканской комиссии гражданской авиации и ИКАО о реализации шести глобальных приоритетных направлений действующего Плана и о том, как обновленный План должен обеспечивать реагирование на новые и эволюционирующие угрозы и риски при безусловном сохранении сильной глобальной системы авиационной безопасности, основанной на эффективности национальных систем безопасности.

В ходе дискуссии обсуждались также вопросы совершенствования национального государственного надзора за обеспечением авиационной безопасности, непосредственно направленного на полную реализацию стандартов ИКАО и целей Глобального плана авиационной безопасности.

Сессия № 4 «Одна цепочка, много участников: модернизация безопасности авиагрузов и почты» с участием спикеров из Казахстана, Еврокомиссии и Ассоциации «Глобал Экспресс» обсудила бурный



Виктор Гулин

рост электронной коммерции, который придал системе перевозок грузов и почты колоссальную гибкость и скорость, но одновременно обнажил новые уязвимости систем безопасности.

Практическим блоком сессии стала презентация Международной ассоциации эксплуатантов (ИАТА), посвященная переходу на электронную декларацию безопасности грузов (CSD/e-CSD) в соответствии с пунктом 4.6.8 Приложения 17 «Авиационная безопасность. Защита международной гражданской авиации от актов незаконного вмешательства» к Конвенции о международной гражданской авиации.

Сессия № 5 «Последний рубеж: кибербезопасность в авиационной системе» обобщила выступления спикеров из Турции, Казахстана, Евроконтроля и ИАТА, акцентировавших внимание на переходе от защиты отдельных авиационных организаций к киберустойчивости всей авиационной системы на основе Стратегии ИКАО по кибербезопасности и соответствующего Плана действий ИКАО.

На фоне активной цифровизации авиационной отрасли обострились задачи защиты критически важных информационных систем аэропортов и авиакомпаний, организации коллективного противодействия кибератакам в целях обеспечения устойчивости авиационной инфраструктуры.

Сессия № 6 «Спорное небо: когда карта меняется за одну ночь» с участием спикеров из США, Франции, Италии и Казахстана обсудила необходимые действия государств и эксплуатантов при возникновении или эскалации конфликтов, рассмотрела также вопросы управления, обмена информацией, реагирования на инциденты и киберугрозы, организации культуры кибербезопасности.

Отмечена острая необходимость быстрого и эффективного обмена информацией о киберугрозах между государствами и в отрасли, своевременных



и обоснованных оценок рисков безопасности и формирование системы проактивной оценки и принятия мер реагирования на новые угрозы и риски.

Сессия № 7 «За пределами бюджетной черты: устойчивая модернизация систем безопасности» заслушала предложения спикеров из Объединенных Арабских Эмиратов, Люксембурга, Казахстана и Европейской комиссии гражданской авиации, представивших свое видение поддержания и развития потенциала авиационной безопасности в условиях ограниченного финансирования, кадров и времени, в том числе подходы к модернизации авиационной безопасности аэропортов при реально доступных ресурсах на основе приоритизации по риск-ориентированному подходу к обеспечению безопасности.

Сессия № 8 «Безопасность – это люди: персонал, компетенции и культура» проходила при участии спикеров из Индии, Омана, Турции и международной организации TADAM и была посвящена человеческому фактору в обеспечении авиационной безопасности. Ключевой посыл: технологии и технические средства дают возможности, но безопасность обеспечивают люди – их решения, внимательность, инициативность, подготовка, культура безопасности, результативность контроля и надзора, готовность сообщать об уязвимостях.

В ходе дискуссии были определены три основных направления для устойчивого обеспечения авиационной безопасности: привлекать и удерживать эффективных сотрудников, оценивать и поощрять реальную результативность работы, формировать и поддерживать принцип персональной ответственности и лидерские качества сотрудников аэропортов, авиакомпаний, подрядчиков и органов власти.

В числе параллельных сессий особое место заняла **сессия по новому поколению авиационных специалистов,** на которой выступили Генеральный секретарь ИКАО Х. К. Саласар, Вице-министр транспорта Республики Казахстан Т. Ластаев, заместитель директора Бюро ИКАО М. Мартин, заместитель директора УАТ ИКАО С. Хифди, региональный директор Европейского и Северо-Атлантического Бюро ИКАО Н. Ралло и представитель Кабо-Верде А. Алмейда.

Отмечено, что кадровое планирование должно охватывать привлечение, подготовку и удержание специалистов с понятными возможностями кадрового роста, включая развитие отраслевой системы наставничества и кадрового резерва с ежегодным мониторингом его результативности.

Особое внимание было уделено вопросам привлечения молодежи в авиационную отрасль, совершенствованию профессионального образования и инновационным методам передачи знаний между поколениями специалистов.

Еще одна параллельная **сессия – «Противодействие несанкционированному использованию беспилотных авиационных систем»** – была проведена совместно Секретариатом ИКАО, Исполнительным директоратом Контртеррористического комитета ООН, Управлением ООН по контртерроризму с привлечением спикеров из управлений ООН, ИКАО, ОАЭ, США и Аргентины и была посвящена обсуждению законодательства, технологических решений и национального опыта по защите объектов авиационной инфраструктуры от актов незаконного вмешательства с использованием беспилотных авиационных систем.

Очень увлекательной и интересной была параллельная **сессия «Сила взгляда: женщины, человеческий фактор и будущее авиационной безопасности»**, в которой участвовали спикеры-женщины из ИКАО, Казахстана, ОАЭ, Италии и Венгрии, обсуждавшие роль женщин как важного звена в системе авиационной безопасности, их особому подходу к распознаванию угроз, взаимодействию с пассажирами и коллегами, а также быстрому принятию решений в кризисных ситуациях. Отмечено, что уникальный женский взгляд на бытовые мелочи

не просто уместен, но в системе безопасности, и особенно профайлинга, играет решающую роль.

Сессия № 9 «Путь к Конференции ИКАО высокого уровня по авиационной безопасности» привлекла спикеров из Эквадора, Грузии и Португалии, которые обсудили пути и вопросы подготовки Конференции ИКАО высокого уровня как площадки для принятия стратегических решений по развитию глобальной системы авиационной безопасности.

На заключительной **сессии «Послания из Астаны»** были подведены итоги всех прошедших на Неделе международных дискуссий и определены основные направления совместной деятельности ИКАО и государств по развитию и укреплению глобальной системы авиационной безопасности в международной гражданской авиации.

В этой сессии выступили Генеральный секретарь ИКАО Хуан Карлос Саласар, Вице-министр транспорта Республики Казахстан **Талгат Ластаев**, Региональный директор Европейского и Северо-Атлантического регионального бюро ИКАО **Николас Ралло** и старший директор по международным отношениям и безопасности Министерства транспорта Сингапура **Бернард Лим**. Они затронули вопросы обеспечения авиационной безопасности в условиях быстро меняющихся угроз, требующих не только ускоренного совершенствования международных стандартов и рекомендуемой практики ИКАО, но и конкретных действий на региональном и национальном уровнях, обмена информацией и современными технологиями при безусловном укреплении сотрудничества и доверия между государствами.

При этом было обращено внимание на то, что ИКАО придает особое значение роли Региональных рабочих групп по авиационной безопасности и упрощению формальностей, внедрению инноваций в обеспечение и надзор за обеспечением авиационной безопасности, развитию и продвижению Универсальной программы ИКАО проверок по авиационной безопасности с использованием механизма непрерывного мониторинга и постоянному повышению компетенций персонала всех уровней в сфере безопасности.



Особо подчеркивалось, что ни одно государство не способно самостоятельно эффективно противостоять всем современным угрозам, особенно киберугрозам, рискам полетов вблизи зон конфликтов и неправомерному использованию беспилотных авиационных систем.

Тотальное применение цифровизации и использование искусственного интеллекта открыли новые возможности в обеспечении безопасности, но и создали новые угрозы, которые еще только предстоит изучить и выработать меры по противодействию им.

«Способность ИКАО и государств предвидеть угрозы и действовать на опережение должна стать привычной практикой, – подчеркнул Генеральный секретарь ИКАО. – Укрепление глобальной авиационной безопасности требует более тесного сотрудничества как внутри государств, так и между ними; взаимодействия различных отраслей, государственных органов, авиационных организаций и международных партнеров. Кроме того, важно помнить, что в основе авиационной безопасности всегда находятся люди. Технологии, нормативные требования и современные системы защиты формируют необходимую основу авиационной безопасности. Однако в конечном счете именно люди обеспечивают их эффективное функционирование».

В ходе Недели руководитель делегации Российской Федерации Виктор Гулин провел ряд двусторонних встреч и бесед, в том числе с руководством Секретариата (штаб-квартиры) и Регионального бюро ИКАО, с руководством Министерства транспорта и авиационной администрации Республики Казахстан.

Главным итогом Недели стало общее понимание того, что дальнейшее совершенствование авиационной безопасности должно основываться на укреплении международного глобального, регионального и двустороннего сотрудничества и способности ИКАО и государств на национальном уровне своевременно адаптироваться к новым угрозам и рискам.

Делегация Российской Федерации, участвовавшая в Неделе ИКАО по авиационной безопасности, с большим успехом представила Россию на международном мероприятии мирового масштаба, в очередной раз показав наши достижения и значимость России в обеспечении авиационной безопасности в международной гражданской авиации. ■

Фото: из личного архива автора

НОВЫЕ ИНИЦИАТИВЫ И ТИРАЖИРУЕМЫЕ РЕШЕНИЯ

Минтранс России запустил конкурсный отбор среди субъектов РФ для участия в формировании низковысотной экономики. Проект реализуется в рамках исполнения поручений Президента России о развитии автономных систем и нацелен на ускоренное внедрение беспилотников в ключевые отрасли экономики страны. Для транспортной отрасли этот пилот – сигнал о переходе беспилотной логистики из стадии экспериментов в стадию реальной коммерческой эксплуатации.



Татьяна Горовая, *председатель Общественного совета при Минтрансе России, первый заместитель генерального директора Центра стратегических разработок*

Именно от того, насколько удастся выстроить экономику, инфраструктуру и межведомственное взаимодействие, зависит, станут ли дроны привычным звеном логистической цепочки в масштабах страны. А смежные инициативы Общественного совета при Минтрансе России – от финансовых механизмов до семейноцентричности – показывают, что повестка выстраивается системно: не только «запустить дрон», но и подготовить инфраструктуру, нормативную базу и общественное восприятие новых транспортных технологий.

РАБОТА С РЕГИОНАМИ

Помимо конкурсного отбора для пилота по БАС, Совет планирует регулярно – раз в квартал – вовлекать общественные советы региональных минтрансов в федеральную повестку. Первое такое мероприятие уже прошло в рамках Исламского форума в Казани. Ожидаемый результат – через региональные общественные организации доносить актуальные вопросы и синхронизировать повестку. До конца года мы планируем с регионами обсудить модели технологического суверенитета, взаимодействие по вопросам информационной безопасности, рекомендации по взаимодействию регионов и бизнеса по вопросам такси, вопросы популяризации безопасности дорожного движения.

СЕМЕЙНОЦЕНТРИЧНОСТЬ

Совет готовит памятку для пассажиров с детьми: на что обратить внимание родителям, какие условия и сервисы доступны, как подготовить ребенка к поездке, что делать, если ребенок потерялся, что должно быть в дорожной аптечке и как действовать при задержке рейса. Материал планируется оформить в виде карточек для публикации на сайтах Совета, Минтранса, Общественной палаты и транспортных компаний. Разработка ведется с участием перевозчиков, вокзалов и общественности. Кроме того, готовится доклад по результатам мониторинга доступности транспортной инфраструктуры для семей с детьми – аэропортов, железнодорожных вокзалов и автовокзалов. Летом Общественная палата при участии Совета провела мониторинг в регионах; готовится доклад с результатами и рекомендациями. Роль Совета – обеспечить достоверную и объективную информацию и адекватные рекомендации. Презентация доклада и обсуждение рекомендаций с представителями транспортных компаний и объектов инфраструктуры пройдут на совместном заседании комиссии ОП РФ и Совета в этом году.

ЭКСПЕРТНАЯ РАБОТА

В рамках «Транспортной недели» запланирована экспертная сессия «Вызовы времени: новые тренды в финансировании транспортных проектов». Участие подтвердили Минэкономразвития, Газпромбанк, ВЭБ, ВТБ, АИИК, консалтинговые компании



Председатель Комиссии ОП РФ по просвещению, воспитанию и защите исторической памяти Ольга Голышенкова, первый заместитель Министра транспорта Российской Федерации Константин Пашков и председатель Общественного совета при Минтрансе России Татьяна Горовая. Совместное заседание Общественного совета при Минтрансе России и Комиссии ОП РФ по просвещению, воспитанию и защите исторической памяти. Москва. 12 августа 2026 г.

в сфере ГЧП, грузоотправители. Ожидаемый результат – рекомендации по текущим рабочим механизмам и изменению законодательства, включая механизм take or pay.

РАБОТА С МОЛОДЕЖЬЮ

При Совете создана межведомственная рабочая группа по патриотическому воспитанию молодежи. Она объединяет молодежные советы ведомств и ряда транспортных компаний. Ожидаемый результат – проведение совместных мероприятий для большего охвата участников, обмен лучшими практиками. Первое заседание уже состоялось, формируется план работы.

ПИЛОТНЫЙ ПРОЕКТ БАС: ЧТО ДАЛЬШЕ

Итоги отбора регионов для пилота по БАС планируется представить в ноябре, в том числе на «Транспортной неделе». После определения участников начнется согласование и заключение соглашений о взаимодействии с субъектами РФ. В рамках «Транспортной недели» также пройдет совместное заседание по вопросам реализации пилота с заслушиванием представителей АИРР, участвующих регионов и отраслевых экспертов.

По итогам проекта предполагается сформировать комплекс организационных, технологических и экономических решений, которые смогут использовать другие регионы при развитии беспилотных грузоперевозок. Полученные результаты также лягут в основу предложений по совершенствованию нормативного регулирования и условий применения БАС. ■

Фото: из личного архива автора, Владимир Дехтеринский, пресс-служба Минтранса Новосибирской области



Совместное выездное заседание Общественного совета при Минтрансе России и профильных общественных советов субъектов Сибирского федерального округа. Новосибирск. 12 марта 2026 г.

МИНТРАНС И ФТС: ОСНОВЫ ПРОДУКТИВНОГО ВЗАИМОДЕЙСТВИЯ

28 октября в Москве состоялась юбилейная конференция Ассоциации содействия участникам ВЭД «Внешнеэкономическая деятельность: открытый диалог», посвященная 10-летию Ассоциации.



Мероприятие объединило около 60 представителей профессионального сообщества, включая руководителей подразделений ВЭД компаний и отраслевых ассоциаций.

Одним из главных событий конференции стал открытый диалог председателя Общественного совета при Минтрансе России **Татьяны Горовой** и председателя Общественного совета при ФТС России **Леонида Лозбенко.**

Участники обсудили эффективность общественных советов, совершенствование таможенного администрирования, развитие транспортной логистики, цифровизацию и механизмы взаимодействия государства и бизнеса.

В работе круглого стола приняли участие члены Общественного совета при Минтрансе России **Вячеслав Керов** и **Сергей Бураго**, руководитель аппарата Общественного совета при Минтрансе России **Анна Болдырева**, член Общественного совета при ФТС России **Галина Донцова**.

Татьяна Горовая, председатель Общественного совета при Минтрансе России:

– Общественные советы создаются и работают сейчас для того, чтобы поддерживать какие-то инициативы и доносить проблемы до профильного



министерства. Безусловно, в общественных советах есть лидеры, те, кто действительно вовлечен в общественную работу. Но, к сожалению, есть люди, которые пришли туда ради пиара. Поэтому с уверенностью могу сказать, что все зависит от лидерских и человеческих качеств членов советов.

Мы стараемся всегда протянуть руку помощи Минтрансу в плане экспертизы документов, которые там готовят, и документов, которые уже приняли, подсказав, где и что нужно доработать, скорректировать. И нас слышат.

Так, мы активно принимали участие в подготовке правил недискриминационного доступа в сфере железнодорожных перевозок, которые действуют в настоящее время. Мы делали соответствующие расчеты, проводили стресс-тестирование результатов, пытались понять, где экономика будет в плюсе, а где в минусе, что будет с бизнесом. Удалось скорректировать тарифы на железнодорожные перевозки. Помогаем готовить законопроект о транспортной политике, чтобы на территории всей страны действовали единые правила и выполнялись единые требования. Минтранс на местах проводит с регионами большую разъяснительную работу, в которой наш общественный совет принимает активное участие. В регионах тоже есть и советы, и общественные объединения, губернаторы и министры регулярно проводят встречи с представителями крупных компаний. И к нам нередко обращаются компании, которые не были приглашены на такие встречи. С помощью Минтранса или сами, когда наших компетенций достаточно, проводим для них мероприятия.

Постоянно актуализируется Транспортная стратегия Российской Федерации. Это коллективный труд с Минтрансом, подведомственными Минтрансу агентствами, службой и организациями.

Приходит очень много точечных запросов от компаний транспортного сектора, и наша задача – помогать находить решения. Когда тема запроса не касается деятельности Минтранса, мы поступаем следующим образом. Я иду в Минтранс, спрашиваю, нет ли никаких противоречий – не занимается ли кто-то параллельно этой работой. Получаю там ответ, и либо мы встраиваемся в уже проводимую работу с нашими инициативами, либо мы получаем мандат на действия самим. Далее, имея нормальные рабочие отношения с другими ведомствами (например, с Минпромторгом или Минэкономразвития), обращаемся в туда и получаем какое-то решение.

Общественный совет при Минтрансе России ценят за то, что мы отделяем лоббизм и индивидуальные



Татьяна Горовая

интересы от действительно системных проблем. Министры всегда знают, что если мы обратились за точечным решением для конкретного предприятия, мы сделаем хорошо не только этому предприятию, но и всем остальным в отрасли. Если мы о чем-то просим, то данный вопрос нами уже отфильтрован и проработан.

Одно из ключевых направлений нашей работы – это, конечно, цифровизация отрасли. Задача экспертного сообщества – помочь найти баланс между внедрением новых технологий и сохранением надежности транспортной системы. Технологии должны повышать эффективность и удобство, но безопасность всегда должна оставаться приоритетом. Поначалу это всегда сложный процесс, но со временем становится понятно, насколько эти технологии полезны, что они дают возможность высвобождения и трудовых, и финансовых ресурсов. Нам от этого не уйти, хотим мы этого или нет. Многие решения принимаются достаточно быстро – и мы бежим, пробуем, спотыкаемся, но тем не менее стараемся эффективно работать в этом режиме. Наша страна одна из лидеров в области цифровизации. Это факт, и это очень здорово.

Что касается взаимодействия с Общественным советом при ФТС России, мы уже договорились, что проведем совместное заседание, подготовим перечень вопросов, пригласим руководителей наших ведомств и вместе будем двигаться вперед. И если какие-то профильные вопросы будут возникать, то решать их будем совместно. Наши ведомства постоянно находятся в достаточно плотных рабочих отношениях: пункты пропуска, цифровизация, данные и т. д. Поэтому мы будем «дружить домами» и продуктивно работать.



Леонид Лозбенко

Леонид Лозбенко, председатель Общественного совета при ФТС России:

– Очень многое зависит от того, кто руководит общественным советом. Мне проще: вся моя жизнь связана с таможней. Я – профессиональный таможенник и хорошо знаю, что происходит в этой сфере в стране и в мире. У нас в ФТС два совета. Задача первого – чтобы служба была одета, обута, экипирована, хорошо снабжена юридически. Второй совет – экспертно-консультативный.

Главная задача таможни на сегодняшний день – обеспечение единообразного применения таможенных правил на всей территории Российской Федерации. Звучит очень общо, но это самое главное. Потому что мне и по сей день представители западных компаний звонят и говорят: «Господин Лозбенко, к вам зайти через Дальний Восток и Калининград – как в две разные страны». И это не потому, что мы так хотим. Дальний Восток, западные границы – везде свои нюансы. Но, с другой стороны, везде таможенные правила должны применяться одинаково.

В таможне есть три базовых вещи – номенклатура, таможенная стоимость и страна происхождения. И я сейчас веду активную работу вместе с руководителем Службы: по этим базовым вещам мы собираем проблемные вопросы. Я обратился к нашим представителям во всех регионах России и попросил поговорить с бизнесменами, спросить, какие у них есть претензии к таможне по этим трем направлениям. Мы их обобщим и постараемся разработать единый алгоритм, чтобы инспектор действовал по нему, а не размышлял о том, что ему делать в каждом случае, и не лез в десятки базы данных.

Могу привести цифру, которая даже меня удивила. Согласно нашим исследованиям, 93% участников внешнеэкономической деятельности на сегодняшний день удовлетворены теми технологическими инструментами, которые применяет таможня. По сравнению с тем, что было, что есть сейчас – это день и ночь. Мы все решаем в цифре. Применяется искусственный интеллект. Президент нам поставил задачу – сократить время нахождения транспортного средства в пункте пропуска на границе до десяти минут. Попробуйте это сделать без внедрения новых технологий, когда задействовано такое количество контролирующих ведомств.

Для нас взаимодействие с Минтрансом на сегодняшний день практически базовая вещь. Без вас, уважаемые коллеги, мы многого сделать не сможем.





Ситуация в мире поменялась, и она будет меняться дальше. Раньше мы все каждый день слышали слово «глобализация». Но после прихода к власти в США Дональда Трампа это слово забыто. Его вообще никто больше не употребляет – ни в других странах, ни у нас. И теперь каждый сам за себя. В этой связи резко возросла роль таможни в мире. Это вполне естественно. Потому что каждая страна защищается. Да, есть союзы, есть блоки, но даже там роль таможни резко возросла.

Мы понимаем свою ответственность. В Службе работает 58 тысяч человек. А всего в мире около миллиона таможенников, которые администрируют 97,5% мирового торгового оборота. Это триллионы и триллионы долларов. Представляете, какая на них лежит нагрузка и какова роль этой системы?

В сентябре Правительство Российской Федерации актуализировало Стратегию развития таможенной службы до 2030 года. Два месяца назад была принята наша новая Единая автоматизированная информационная система таможенных органов второго поколения – ЕАИС ТО 2.0. Мы планируем очень многое сделать в следующем году. Все подготовили для этого. Нас поддержали Президент и Председатель Правительства. Поддержал наш куратор, заместитель Председателя Правительства Российской Федерации – Министр финансов Российской Федерации Антон Силуанов. Его назначение на должность вице-премьера для нас большая радость, потому что повышается уровень взаимоотношений с другими ведомствами.

Хочу еще раз подчеркнуть, таможня – удивительная структура. Потому что все ведомства, включая



Минтранс, выстроены по вертикальному принципу, а таможня – по горизонтальному. Времена меняются, и роль Службы сегодня резко возрастает. Мы это чувствуем, мы это видим, мы это четко понимаем. К сожалению, должен признать, что количество уголовных и административных дел с годами не уменьшается. Не буду называть цифры, они очень большие. Все понимают: страна воюет. Но далеко не все понимают, что и как надо делать в рамках закона. Поэтому обращаюсь к присутствующим уважаемым представителям крупных компаний: постарайтесь работать так, чтобы у нас к вам не было претензий. Убежден, что мы этого добьемся вместе.

Александр Никитушин. Фото: Александр Падежов

ОТ ДАННЫХ – К РЕШЕНИЯМ

Директор ФГБУ «СИЦ Минтранса России» Александр Кисляков – о том, как СИЦ Минтранса России развивает цифровые решения для управления транспортным комплексом.



Александр Кисляков,
директор ФГБУ «СИЦ Минтранса России»

– Александр Валерьевич, СИЦ Минтранса России работает сразу по нескольким направлениям: от государственных информационных систем до мониторинга транспортной ситуации и развития сервисов для граждан. Какую основную задачу решает Центр сегодня?

– СИЦ Минтранса России обеспечивает информационно-аналитическую поддержку управления транспортным комплексом, развивает отраслевые цифровые системы и помогает формировать единое информационное пространство транспортной отрасли. За последние годы профиль Учреждения существенно изменился. К организационно-техническому обеспечению и мониторингу добавились задачи в области цифровизации, работы с данными и создания государственных информационных систем. Сегодня мы объединяем технологические решения, отраслевые данные, ситуационный мониторинг и аналитику.

Наша задача – сделать все, чтобы эта работа давала практический результат: помогала принимать управленческие решения, повышать безопасность перевозок, развивать инфраструктуру и делать транспортные услуги удобнее для граждан и бизнеса.

– Как эта работа отражается на управлении транспортным комплексом?

– Чем полнее картина происходящего, тем быстрее можно оценить ситуацию, определить масштаб проблемы и организовать реагирование. Эту задачу решает, в частности, информационно-аналитическая система регулирования на транспорте (АСУ ТК). В режиме реального времени она обеспечивает учет данных об инцидентах и функционировании объектов транспортной инфраструктуры, а также координирует реагирование на сбойные ситуации. В данный момент система функционирует в пилотном режиме, и наши специалисты дорабатывают ее обновленную версию по результатам эксплуатации.

В 2026 году на базе СИЦ Минтранса России создан Единый центр управления транспортным комплексом – ЕЦУ ТК. Как отметил Министр транспорта России Андрей Никитин на Правительственном часе в Совете Федерации, данный Центр объединяет ситуационные центры всех видов транспорта во всех регионах страны. Сейчас СИЦ активно занимается его развитием, делая функционирование транспортного комплекса и управление им более эффективным.

– Какие изменения в работе Центра можно выделить по приблизительным итогам 2026 года?

– В этом году мы продолжаем расширять цифровые инструменты и развивать системы, которые помогают решать задачи транспортной отрасли. Одним из ключевых результатов стало, как уже было упомянуто, создание ЕЦУ ТК. Центр формирует единую информационную основу для ситуационного управления транспортным комплексом. Еще одно важное направление работы – расширение регионального охвата и повышение оперативности получения информации. Например, уже сейчас в информационное поле ЕЦУ ТК включены 58 субъектов РФ, взаимодействие с которыми осуществляется на основании заключенных соглашений. Это позволяет региональным министерствам транспорта видеть все

нештатные ситуации на территории субъекта, отслеживать их и оперативно устранять последствия. Такой подход важен как для обеспечения безопасности и устойчивой работы транспортной инфраструктуры, так и для снижения экономических последствий транспортных сбоев: сокращения времени простоя, ограничения перевозок и нарушения логистики.

А формировать единую картину транспорта в субъектах РФ успешно помогает Цифровой профиль региона (ЦПР). На сегодняшний день все 89 субъектов успешно подключены к системе, анализирующей степень внедрения цифровых технологий в транспортном комплексе.

В составе цифровых решений Центра также развивается Цифровая система управления строительством транспортных объектов (ЦУС), входящая в контур АСУ ТК. Ее уникальность заключается в следующем: система призвана сформировать единую доверенную цифровую среду для управления строительством транспортной инфраструктуры, охватывающую все уровни отрасли – от рядовых работников на строительных площадках до руководства Минтранса России.

Еще одним значимым событием стало официальное назначение СИЦ Минтранса России оператором НЦТЛП «ГосЛог». Соответствующий приказ Министр транспорта России Андрей Никитин подписал в июле этого года. На Учреждение возложены полномочия оператора платформы и ее эксплуатации.

Отдельное направление – развитие социально значимых сервисов. Например, АИС УЛСП позволяет подтверждать право граждан на соответствующие меры поддержки в цифровом формате. В 2026 году благодаря развитию системы расширились возможности подтверждения права на льготы при пассажирских перевозках. С февраля подтвердить статус члена многодетной семьи при бронировании субсидированных авиабилетов стало доступным не только в «Аэрофлоте», но и в S7. Это позволило сократить время подтверждения права на льготу с пяти рабочих дней до нескольких минут и отказаться от бумажных справок.

АИС УЛСП также стала технологической основой нового механизма предоставления скидок на парковку в аэропорту Шереметьево для многодетных семей: право на скидку в размере 25% проверяется автоматически по номеру СНИЛС при оформлении услуги онлайн. Кроме того, система обеспечила возможность подтверждения льготного статуса с помощью цифрового ID в национальном мессенджере «МАКС»: соответствующий сценарий доступен студентам для льготного проезда в пригородных поездах и внедрен в общественном транспорте в 87 субъектах РФ.

Еще одним направлением развития системы стал экспериментальный запуск в Республике Башкортостан проекта «Моя карта «Мир»», реализуемого совместно с Национальной системой платежных карт (НСПК). Проект позволяет оплачивать льготный проезд банковской картой без оформления отдельного проездного. АИС УЛСП обеспечивает технологическую основу проекта, объединяя данные о маршрутах и зонах действия транспортных льгот, а взаимодействие с платформой НСПК позволяет





Стратегическая сессия ФГБУ «СИЦ Минтранса России». РУТ (МИИТ). 11 сентября 2026 г.

настраивать региональные льготные программы. Для получения льготы пассажиру достаточно привязать карту «Мир» на портале «Госуслуги». Поездки оплачиваются по обычному тарифу, пока их суммарная стоимость за месяц не достигнет стоимости льготного проездного – в Башкортостане это 600 рублей. После этого поездки становятся бесплатными до конца месяца в пределах лимита в 90 поездок.

В 2026 году СИЦ также подписал соглашение об информационном взаимодействии с авиакомпанией «Аврора» для ее последующей интеграции с АИС УЛСП. Это позволит пассажирам оформлять субсидированные билеты онлайн с автоматическим подтверждением права на льготу. Запуск технологии для региональных спецтарифов запланирован на начало 2027 года и станет первым опытом подтверждения региональных льгот на Дальнем Востоке.

Продолжается и развитие ФГИС «Такси». Система обеспечивает работу с данными о перевозчиках и транспортных средствах, а также позволяет пассажирам проверять легальность перевозчика. В 2026 году развивается взаимодействие с национальным мессенджером «МАКС», в том числе ведется разработка сценария проверки такси по фотографии государственного регистрационного номера или его ручному вводу.

СИЦ также оказывает помощь ветеранам СВО, гражданам и бизнесу, предоставляя информацию и обеспечивая поддержку по вопросам транспортного комплекса. У нас функционируют две горячие линии: по вопросам транспортной логистики на Крымском мосту и для участников СВО и их семей, и уже зафиксировано более 200 обращений. В том числе в этом году стало доступно сопровождение сухопутного альтернативного маршрута, карту проезда по которому можно найти на сайте нашего Учреждения.

– Центр занимается не только разработкой цифровых систем, но и мониторингом функционирования объектов транспортной инфраструктуры, а также чрезвычайных и нештатных ситуаций. Насколько удалось повысить оперативность работы?

– Для ситуационного управления время получения и обработки информации имеет принципиальное значение. Поэтому мы последовательно совершенствуем процессы, автоматизируем обмен данными и выстраиваем взаимодействие с профильными ведомствами. Например, уточнение сведений о чрезвычайных ситуациях теперь занимает три минуты вместо десяти – это в три раза быстрее. Совместно с Росавиацией мы также перестроили процесс информирования: руководство Минтранса России получает данные об авиационных инцидентах напрямую, в течение 10 минут с момента подачи сигнала пилотам. Это позволяет получать информацию в шесть раз быстрее. Чем быстрее удается оценить ситуацию и принять необходимые меры, тем выше возможности сократить время простоя транспорта и инфраструктуры, минимизировать задержки перевозок и связанные с ними экономические потери.

В конечном счете оперативный обмен информацией помогает поддерживать устойчивость транспортных процессов и снижать последствия нештатных ситуаций для участников отрасли.

– В этом году прошла первая стратегическая сессия СИЦ с участием представителей Минтранса России, специального представителя Президента Российской Федерации по вопросам цифрового и технологического развития, государственных органов, экспертного сообщества и РУТ (МИИТ). Расскажите, как было принято решение о проведении подобного мероприятия и какие вопросы были подняты для обсуждения.

– СИЦ значительно вырос: расширились направления деятельности, появились новые проекты и компетенции, увеличилась команда. Мы научились эффективно выполнять поставленные задачи и синхронизировать работу разных подразделений. Теперь необходимо было определить, как объединить накопленный опыт и возможности в единую систему развития. Стратегическая сессия стала площадкой для обсуждения будущего Учреждения и его роли в цифровой трансформации транспортной отрасли. Мы рассмотрели вопросы развития работы с данными, платформенных решений, ситуационного управления, информационного сопровождения и подготовки кадров.

Обсудили также один из следующих этапов работы – внедрение предиктивной аналитики, которая позволит прогнозировать масштаб влияния инцидентов и сроки восстановления. Это позволит органам управления проводить превентивные и оперативные мероприятия, что поспособствует минимизации последствий и существенно сократит экономические потери.

Одним из ключевых ориентиров стало усиление роли СИЦ как оператора отраслевых данных. Этот вектор обозначил первый замминистра транспорта Константин Пашков – мы стремимся к тому, чтобы стать «цифровым продолжением Минтранса». Для этого необходимо выстраивать системный сбор актуальной и проверенной информации, развивать аналитику и обеспечивать ее использование при принятии решений. Еще одно направление – переход от отдельных информационных систем к согласованной архитектуре цифровых платформ.

Отдельное внимание мы уделяем взаимодействию между подразделениями и сотрудничеству с РУТ (МИИТ). Развитие цифровых решений требует не только технологий, но и сильных команд, общих стандартов работы и подготовки специалистов, понимающих специфику транспортной отрасли.

– Какие задачи Центр ставит перед собой на ближайшую перспективу?

– Среди ключевых задач – развитие ЕЦУ ТК, внедрение инструментов предиктивной аналитики и искусственного интеллекта, совершенствование ФГИС «Такси», НЦТЛП «ГосЛог», АИС УЛСП и других цифровых решений.

Мы последовательно смещаем акцент с мониторинга инцидентов в режиме реального времени на прогнозирование рисков, способных повлиять на работу транспортного комплекса и его экономические показатели. Это позволит заблаговременно выявлять потенциальные угрозы, оценивать возможные последствия и принимать решения для их предотвращения, повышения устойчивости и экономической безопасности отрасли.

Важная задача – повышать ценность данных, которыми располагает Центр. Мы стремимся к тому, чтобы каждый показатель приносил больше пользы, а данные о состоянии и функционировании транспортного комплекса становились содержательнее для специалистов, руководителей и участников транспортно-логистических процессов.

Еще одно направление – усиление кибербезопасности. В перспективе соответствующие инструменты могут быть интегрированы в обновленную АСУ ТК в качестве отдельной подсистемы. Это позволит учитывать киберугрозы в общей системе мониторинга и при выявлении инцидентов оперативно передавать необходимую информацию ответственным специалистам.

Также задача СИЦ – синхронизировать действия всех подведомственных организаций транспортного комплекса, используя цифровые инструменты не только для оперативного мониторинга и получения информации о состоянии отрасли, но и для координации совместных действий и повышения эффективности управленческих решений.

В целом мы движемся от фиксации чрезвычайных ситуаций и нештатных событий к комплексному мониторингу в режиме реального времени, прогнозированию рисков и оценке их возможного влияния в том числе на экономические показатели транспортного комплекса. Для нас важно, чтобы цифровые решения помогали видеть происходящее и заранее определять, где могут возникнуть проблемы и какие меры позволят минимизировать их последствия для пассажиров, логистики и всего транспортного комплекса.

Беседовал Вячеслав Керов

Иллюстрации: пресс-служба Минтранса России

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ ВОЗДУШНОГО ТРАНСПОРТА



Сергей Половников,
руководитель рабочей группы по вопросам категорирования объектов критической информационной инфраструктуры Комиссии по вопросам транспортной безопасности и безопасности на транспорте Общественного совета при Минтрансе России

На текущий момент требования Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» предусматривают обязательную процедуру категорирования объектов критической информационной инфраструктуры (далее – КИИ), в том числе субъектов транспортной отрасли и объектов, которые функционируют на воздушном транспорте.

Для организаций воздушного транспорта процедура категорирования, импортозамещения и обеспечения безопасности объектов КИИ всегда была очень чувствительной. С одной стороны, это информационные системы, которые имеют критическое значение для функционирования, с другой стороны, это, как правило, информационные системы, которые очень тесно интегрированы в производственную цепочку.

Тем не менее, все субъекты транспортной отрасли, относящиеся к воздушному транспорту, а это и авиакомпании, и аэропорты, должны пройти процедуру категорирования объектов КИИ в соответствии с существующими правилами, которые регулируются постановлением Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

В феврале 2026 года было принято распоряжение Правительства РФ №360-р «О безопасности критической информационной инфраструктуры», согласно которому был утвержден перечень типовых отраслевых объектов КИИ.

Данным распоряжением утвержден перечень типовых отраслевых объектов КИИ для всех отраслей экономики РФ. К отрасли транспорта, согласно данному перечню, относятся 62 типовых объекта КИИ. В том числе 14 типовых объектов КИИ относятся непосредственно к воздушному транспорту.

К типовым объектам КИИ, воздушного транспорта относятся:

- информационные системы (далее – ИС), автоматизированные системы управления (далее – АСУ), информационно-телекоммуникационные сети (далее – ИТС) управления аэропортом;
- ИС оформления воздушных перевозок;
- ИС, АСУ, ИТС организации перевозок;
- ИС, АСУ, ИТС управления воздушным транспортом;
- ИС, АСУ, ИТС планирования использования воздушного пространства;
- ИС, АСУ, ИТС обеспечения авиационной связи;
- ИС, АСУ, ИТС сбора данных о метеорологической обстановке;
- ИС, АСУ, ИТС регистрации и измерения коэффициента сцепления взлетно-посадочной полосы (далее – ВПП);
- ИС, АСУ, ИТС управления топливозаправочным комплексом;
- ИС, АСУ, ИТС управления электросветотехническим оборудованием;
- ИС, АСУ, ИТС сбора данных (аэронавигация, состояние ВПП, справочная информация);
- ИС, АСУ, ИТС автоматизированного контроля воздушных судов (далее – ВС) (за исключением неотделимых от ВС);

- ИС, АСУ, ИТС радионавигации ВС (за исключением неотделимых от ВС);
- ИС, АСУ, ИТС управления ВС (за исключением неотделимых от ВС).

Соответственно, проведение процедуры категорирования организациями транспортной отрасли и непосредственно организациями воздушного транспорта обязательно должно проводиться с учетом данного типового перечня объектов КИИ. Повторюсь, что руководствоваться данным перечнем – это обязательная процедура, поскольку данный типовой перечень объектов КИИ носит не рекомендательный характер, а обязательный. По результатам проведения процедуры категорирования комплект документов подается в ФСТЭК России, как регулятору в данной области.

СУЩЕСТВУЮЩАЯ ПРАКТИКА

На сегодняшний момент в реестре Росавиации находится 123 организации, осуществляющих коммерческие перевозки воздушным транспортом, 381 организация, имеющая сертификат на выполнение авиационных работ, и 86 организаций, имеющих свидетельство эксплуатанта авиации общего назначения. Помимо этого к воздушному транспорту относятся 226 аэропортов (аэродромов), согласно реестру Росавиации. То есть порядка 350 организаций, имеющих отношение к воздушному транспорту, должны обязательно пройти процедуру категорирования. Определенная динамика в категорировании организаций воздушного транспорта есть, но на сегодня она крайне недостаточная. И, конечно, в данном вопросе организациям воздушного транспорта необходимо ускориться.

Также хотелось бы уделить внимание некоторым из типовых объектов КИИ, а именно – ИС, АСУ, ИТС автоматизированного контроля ВС; ИС, АСУ, ИТС радионавигации ВС; ИС, АСУ, ИТС управления ВС. Ранее ряд авиакомпаний провел процедуру категорирования данных систем до вступления в силу распоряжения Правительства РФ № 360-р. Соответственно, что касается именно данных объектов КИИ, я бы посоветовал этим авиакомпаниям провести процедуру перекатегорирования с учетом требований распоряжения.

Еще несколько слов о типовом объекте – ИС, АСУ, ИТС управления электросветотехническим оборудованием. Это светосигнальное оборудование аэропорта, и на сегодняшний день данная система категорирована в ряде крупных и региональных аэропортов. Она, по сути, является ИТС, и, к сожалению, сегодня полноценные отечественные аналоги отсутствуют. Минтранс России и ФГУП «ЗащитаИнфоТранс», совместно с Росавиацией и ее подведомственной организацией ФГУП «АГА (А)», а также с привлечением отечественных производителей ведут работу по формированию отечественного программно-аппаратного комплекса светосигнального оборудования. Пока есть объективные организационные вопросы, которые требуют решения: замена такого комплекса светосигнального оборудования аэропорта – это существенные затраты, которые необходимо найти и спланировать; также нужно решить технологические вопросы модернизации данного комплекса без остановки деятельности аэропорта.

РОЛЬ ОТРАСЛЕВЫХ ЦЕНТРОВ КОМПЕТЕНЦИЙ

Конечно, при проведении процедуры категорирования объектов КИИ организациями транспорта возникает множество организационных и технических вопросов. Очень часто эти вопросы связаны с недостатком ресурсов на местах, необходимостью разъяснения требований законодательства применительно к конкретным ситуациям, реорганизационными преобразованиями самих организаций транспорта.

С 2022 года на базе ФГУП «ЗащитаИнфоТранс» осуществляет свою деятельность Отраслевой центр компетенций, который помогает всем организациям транспортной отрасли в вопросах категорирования, технологической независимости.

На базе Отраслевого центра компетенций работает горячая линия по поддержке всех организаций транспортной отрасли по вопросам категорирования, импортозамещения ПО, перехода на использование доверенных ПАК, ведется вся аналитическая работа по текущему уровню категорирования и технологической независимости транспортной отрасли. Любая организация транспорта может обратиться в Отраслевой центр компетенций по телефону или электронной почте и получить полную консультацию, запросить шаблоны необходимых документов по озвученным выше вопросам.

В заключение хочу сказать, что объективных сложностей к проведению процедуры категорирования со стороны организаций транспорта нет. Очень часто присутствуют нежелание самих организаций и другие приоритеты в их деятельности, когда есть более важные задачи. Но я бы хотел постараться донести до всех организаций: коллеги, не откладывайте процедуру категорирования объектов КИИ, это ваша инфраструктура, это ваш бизнес и это ваши производственные процессы, которые необходимо защищать и обеспечивать непрерывность работы.

Контакты Отраслевого центра компетенций: ock@z-it.ru; +7 (495) 380-21-50, доб. 200

Фото: Владимир Дехтеринский

«АВИАКОД 2026» И ЦИФРОВАЯ УСТОЙЧИВОСТЬ ГРАЖДАНСКОЙ АВИАЦИИ

Проверка защищенности, контроль подрядчиков и переход на отечественные технологии стали ключевыми темами конференции «Авиакод 2026». Участники обсуждали, как развивать цифровую инфраструктуру авиации, сохраняя надежность ее повседневной работы.



Сергей Левашов, *заместитель генерального директора по информационным технологиям и цифровой трансформации ФГУП ГосНИИ ГА*

8 октября 2026 года в Москве прошла научно-практическая конференция «Авиакод: новые стандарты и передовые ИБ-решения для авиации». Мероприятие собрало 230 представителей авиационной отрасли. Организаторами выступили ФГУП ГосНИИ ГА и ООО «СТАФФСОФТ». В обсуждениях участвовали представители государственных органов, научных организаций и российских разработчиков. Наряду с деловой программой работала выставка цифровых решений и средств информационной безопасности.

По мере цифровизации все больше рабочих процессов авиапредприятий зависит от доступности информационных систем и достоверности данных. Поэтому оценивать защищенность необходимо с учетом последствий возможных сбоев для деятельности предприятия. Такой подход связывает задачи специалистов по информационной безопасности с ответственностью руководителей за непрерывность работы.

ПЛЕНАРНАЯ СЕССИЯ И ПРОВЕРКА ЗАЩИЩЕННОСТИ

Пленарную сессию, посвященную государственному регулированию и киберугрозам в авиационной отрасли, провел заместитель генерального директора ГосНИИ ГА по информационным технологиям и цифровой трансформации **Сергей Левашов**.

Председатель Комиссии по вопросам транспортной безопасности и безопасности на транспорте Общественного совета при Минтрансе России **Вячеслав Керов** представил деятельность Совета в области информационной безопасности транспортной инфраструктуры. Его выступление дополнило обсуждение государственного регулирования и киберугроз, ставшее основной темой пленарной сессии.

Представитель ФСТЭК России **Елена Торбенко** обратила внимание на объективную оценку защищенности, правильное определение границ защищаемого контура и контроль доступа подрядчиков. В прикладных выступлениях обсуждались аудит, тестирование на проникновение и работа центров мониторинга и реагирования на инциденты – SOC.

Отдельное внимание участники уделили внешним специалистам, обслуживающим инфраструктуру. В числе рассматривавшихся мер – требования безопасности в договорах, разграничение полномочий, контроль привилегированного доступа и удаленного управления. Директор Отраслевого центра компетенций по информационной безопасности ФГУП «ЗащитаИнфоТранс» **Сергей Страхов** подчеркнул значение согласованной работы ИТ- и ИБ-подразделений.





ПЕРЕХОД НА РОССИЙСКОЕ ПО

Переходу на российское программное обеспечение был посвящен круглый стол об отказоустойчивой ИТ-инфраструктуре. Представители отрасли назвали основные сложности: территориальную распределенность объектов, необходимость поддерживать производственные процессы во время миграции и дефицит подготовленных кадров.

Руководитель службы информационных технологий ФГУП «Госкорпорация по ОрВД» **Валерий Стецевич** рассказал о комплексной замене иностранного ПО, проводимой с 2022 года. Технический переход сопровождается обучением сотрудников совместно с разработчиками. Этот опыт показывает значение пользовательских навыков: новое решение должно стать полноценным рабочим инструментом для персонала.

В ходе дискуссии прозвучали предложения выработать единые архитектурные принципы, определить рекомендованные решения и организовать отраслевой полигон для пилотных проектов. Инициативу испытательной площадки поддержали участники от «Аэропроекта». Такая площадка позволила бы проверять совместную работу продуктов и накапливать опыт до их широкого внедрения.

Действующий экспертный совет на площадке ГосНИИ ГА служит основой для профессионального взаимодействия авиационных предприятий и разработчиков. Его работа позволяет продолжать обсуждение отраслевых задач между конференциями и обмениваться опытом применения технологий.

ЗАЩИТА НОВЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Искусственный интеллект рассматривался одновременно как средство поддержки специалистов и фактор развития киберугроз. В программе обсуждались интеллектуальная поддержка SOC и безопасное использование ИИ в рабочих задачах. Секция беспилотных авиационных систем охватила защищенные платформы, безопасность связи и предотвращение перехвата управления. Эти направления расширяют круг задач, которые предстоит решать отрасли. При внедрении технологий потребуется заранее определять условия их безопасного применения, ответственность участников и способы проверки результата. Для авиационного предприятия критерием успешной модернизации становится способность инфраструктуры устойчиво выполнять свои функции при штатной эксплуатации, технических изменениях и возникновении инцидентов.

Практический смысл обсуждений на «Авиакод 2026» – в необходимости оценивать защиту вместе с условиями эксплуатации систем. Предприятию важно знать, кто получает доступ к инфраструктуре, как контролируются его действия и какие процессы остаются уязвимыми. Результаты проверок должны помогать руководству определять необходимые изменения и оценивать их влияние на работу организации.

Цифровая устойчивость авиации складывается из проверенной защиты, управляемого доступа и готовности людей работать с новыми технологиями. ■

Фото: Мария Мурашова

ЗАЩИТА ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В АВИАЦИИ



8 октября в рамках деловой программы конференции «Авиакод», посвященной актуальным вопросам цифрового развития гражданской авиации, прошла пленарная сессия «Государственное регулирование и киберугрозы в авиационной отрасли».

Модератором пленарной сессии выступил заместитель генерального директора по информационным технологиям и цифровой трансформации ФГУП ГосНИИ ГА **Сергей Левашов**. Участники дискуссии обсудили изменения законодательства Российской Федерации для субъектов критической информационной инфраструктуры авиационной отрасли, деятельность отраслевого центра компетенций по информационной безопасности транспортного комплекса и работу Общественного совета при Минтрансе России по направлению «Информационная безопасность объектов транспортной инфраструктуры».

В начале своего выступления начальник управления ФСТЭК России **Елена Торбенко** напомнила о последних нововведениях в законодательство: «В ноябре прошлого года были внесены изменения в процедуру категорирования, в этом году – в приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». До конца года мы приступим к обсуждению изменений приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»».

Она озвучила не самую позитивную статистику выполнения требований законодательства в транспортной отрасли в целом и в авиации в частности: «Вместе с отраслевым регулятором мы выбрали более 400 первичных организаций в авиационной сфере. К сожалению, только 60% из них приступило к фактической реализации требований законодательства. Завершили категорирование около половины. Лишь 116 организаций определили у себя значимые объекты. Более чем 200 организациям только



Сергей Левашов

в течение этого года было направлено требование о необходимом выполнении законодательства. Это документ, который обязателен к исполнению: за несоблюдение сроков, установленных в нем, предусмотрена ответственность. Поэтому в отношении порядка 20% этих организаций возбуждены административные дела, как центральным аппаратом, так и территориальными органами. В 18 организациях, которые мы проверили в текущем году, мы выявили более 200 нарушений обязательных требований законодательства. При этом более половины из них не касаются документарной проверки, это не категорирование, с которым тоже, как я сказала, есть проблемы. Это фактические требования, которые не выполняет субъект, что может быть следствием ослабления контроля за работниками, которые причастны к эксплуатации значимых объектов. В отношении этих 18 организаций заведено около 30 административных дел».

Елена Торбенко назвала проблемой наличие программного обеспечения, стоящего на рабочих местах не только пользователей, но и администраторов систем и специалистов по безопасности, администрирующих средства безопасности субъектов, которое не используется в их непосредственной деятельности: «Например, Telegram. Это ПО уязвимое, это ПО, которое взаимодействует с интернетом, а значит, через него во внутренние сети могут спокойно зайти и все системы находятся под угрозой. Вывод: нужно усиливать работу на этом направлении».

Она отметила, что инциденты, которые происходят в большинстве случаев успешно, в том числе в авиационной отрасли, связаны с работой с подрядчиками: «Не секрет, что зачастую работу с системами ведут подрядные организации. И, как правило, это ИТ-организации, которые функционируют в удаленном формате. В 90% проверенных подрядных организаций мы выявили нарушения у сотрудников, которые имеют доступ к значимым объектам, как к прикладным, так и к системам безопасности. Это бич для авиакомпаний и аэропортовых инфраструктур. Необходимо усиливать работу с подрядными организациями и контроль за работой своих систем. Это нужно делать и в рамках документарного обеспечения, то есть договорных отношений, устанавливать соответствующие требования и права службы безопасности субъекта. Нередко с подрядными организациями работают только айтишники, а безопасники к ним не могут зайти. Но когда подряд с личного рабочего места под неограниченными пользовательскими правами администрирует систему, параллельно что-то делая в интернете, у нас возникает вопрос – насколько безопасна такая система и стоит ли вообще ее защищать».

«Работа с уязвимостями должна строиться так: выявление, устранение и повторный анализ, в результате которого можно сделать вывод о том, что уязвимость либо неактивна, либо она неактуальна, – продолжила Елена Торбенко. – У кого-то это отлаженный процесс. У кого-то это отдано опять-таки на усмотрение подрядных организаций, и уязвимости продолжают висеть в системах довольно долго. Для организаций транспортной отрасли разработан ряд дополнительных мер, связанных именно



Сергей Страхов, Елена Торбенко и Вячеслав Керов



с вопросами устранения уязвимостей, в том числе уязвимостей нулевого дня (которые мы еще не публикуем в банке данных угроз), либо с дополнительной настройкой средств безопасности для нейтрализации этих уязвимостей. Мы видим, что зачастую эти мероприятия не проводятся или проводятся недостаточно быстро и эффективно. Поэтому нужно усиливать контроль подрядных организаций за выполнением этой работы. И, конечно, нужно правильно и внимательно проанализировать, какие базовые меры реализуются в системе. Потому что есть значимые объекты, к которым предъявляются обязательные требования, а есть незначимые, но с которыми взаимодействуют значимые системы. Защищать общий периметр систем, когда невозможно их разделить, надо обязательно, реализовывая хотя бы базовые меры».

Для решения выявленных проблем был издан приказ ФСТЭК России от 16.07.2026 № 220 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235», согласно которому в рамках контроля состояния безопасности значимых объектов критической информационной инфраструктуры должны рассчитываться:

- показатель, характеризующий текущее состояние обеспечения безопасности значимых объектов критической информационной инфраструктуры и степень его соответствия минимально необходимому уровню обеспечения безопасности от типовых актуальных угроз безопасности информации (показатель защищенности);
- показатель, определяющий достаточность и эффективность проведенных мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (показатель уровня зрелости).

«С 1 марта 2027 года рассчитывать показатель защищенности по нашей методике будет обязательно для всех субъектов, владеющих значимыми объектами. Рекомендую это делать и для остальных систем. Советую не ждать, а провести оценку сейчас и понять, где, на каком направлении нужно будет докручивать. Когда он станет обязательным, за невыполнение данного требования будет предусмотрена ответственность, – обратилась к присутствующим в зале представителям субъектов Елена Торбенко. – Показатель уровня зрелости также будет введен с 1 марта 2027 года в качестве обязательного для подрядных организаций, для того чтобы вы могли оценить, насколько ваши подрядчики готовы оказывать вам качественные и безопасные услуги. Рассчитываться он будет также по методикам, которые опубликованы

на нашем сайте. С ними можно ознакомиться уже сейчас и применить либо к своим подразделениям, либо к подрядным организациям».

«Не нужно опасаться обращаться непосредственно к регулятору и аттестованным организациям за помощью – стоит там открыть карты и решить свой вопрос. Это гораздо лучше воспринимается регулирующими органами, нежели попытки скрыть какую-то назревшую проблему или не придавать ей значения», – добавил Сергей Левашов и поинтересовался у Елены Торбенко, встречается ли ФСТЭК России с применением искусственного интеллекта для обеспечения информационной безопасности, защиты периметра.

«Конечно, но пока что, в основном, данную технологию применяют в тестовом контуре, хотя кто-то смело внедряет ИИ в продуктивный контур, – ответила она. – Прежде всего, нужно понимать, насколько вы доверяете технологиям, которые внедряете, на чем они основывались, и кто их контролирует. Соответствующие обязательные требования и рекомендации по применению и защите от применения искусственного интеллекта опубликованы в рамках приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Не стоит забывать, что полностью доверять искусственному интеллекту и тем результатам, которые вы получаете, нельзя. То есть периодическая перепроверка результатов должна быть. Также остается открытым вопрос взаимодействия и совместимости с вашими системами».

Отвечая на вопрос об организации технической поддержки используемого российского программного обеспечения, Елена Торбенко отметила, что тема перехода на отечественное ПО с точки зрения безопасности стала крайне актуальной в 2022 году, когда многие технические средства, потеряв поддержку, превратились в «кирпичи». «Техподдержка для средств защиты обязательна. Если мы видим уязвимое прикладное средство, а с 2023 года к прикладным средствам, которые установлены на значимых объектах, тоже есть определенные требования (п. 29.3 приказа ФСТЭК России № 239), то это мы тоже фиксируем. Если там есть уязвимости, которые могут быть проэксплуатированы, то мы соответствующие требования в предписание вносим. Это будет нарушением законодательства», – констатировала она.

Директор Отраслевого центра компетенций по информационной безопасности ФГУП «ЗащитаИнфоТранс» **Сергей Страхов** сообщил, что, согласно полученным данным, более 40% активных угроз, которые были успешно реализованы, связаны с действиями подрядных организаций: «Я прекрасно понимаю, что эксплуатация отдельных информационных систем без привлечения сторонних организаций невозможна. Но здесь надо соблюдать максимальную стерильность. Контроль за представителями



подрядчика должен быть организован на высшем уровне».

Он также согласился с тем, что многие организации плохо работают над устранением уязвимостей: «Часто мы наблюдаем достаточно легковесное отношение к этому вопросу. В ходе аналитических проверок, проводимых по поручению Министерства транспорта, мы фиксируем уязвимости, которые на периметре информационных систем предприятий «живут» годами!»

Сергей Страхов рассказал о готовящемся к запуску портале, где будут публиковаться реализованные и предотвращенные угрозы в транспортной отрасли: «Это будет глобальный проект под эгидой Минтранса России. Предприятия, подключившиеся к данной информационной системе, смогут получить техническую и методологическую поддержку по вопросам обеспечения безопасности. Новый портал Отраслевого центра компетенций по информационной безопасности должен стать площадкой для обмена опытом и, условно говоря, базой знаний для предприятий».

Коснувшись темы методик контроля подрядчиков, он подчеркнул, что универсальной таблетки не бывает: «Предприятия разные, подрядчики разные. Но некоторые предприятия отрасли, особенно крупные (например те, кто занимается грузоперевозками в сфере железнодорожного транспорта, или логистические компании) широко практикуют выездные проверки подрядчиков. В том числе с привлечением нас в качестве отраслевой экспертизы. Мы выезжаем на объекты подрядчиков и смотрим, как реализуются нормативные требования. Понятно, что может быть создан показной эффект, но, по крайней мере, это в любом случае стимулирует подрядчика – он понимает, что находится под присмотром».

«Что касается технических мероприятий, они не новы. В первую очередь используются PAM-системы для контроля за действиями пользователей с расширенными правами, потому что подрядчики, естественно, их получают, – продолжил Сергей Страхов. – Большинство реализованных атак связано с тем, что к нам в инфраструктуру попадает условно неизвестный нам человек, который имеет привилегированный доступ. И это, безусловно, проблема. Некоторые организации проводят сегментирование инфраструктуры. Для подрядчика выделяется небольшой изолированный сегмент, и он получает





доступ к ограниченному набору ресурсов, который не содержит критических данных или уязвимостей. В остальной части инфраструктуры организация проводит работы собственными силами. Да, на это приходится тратить много ресурсов, но зато такой подход максимально обеспечивает безопасность инфраструктуры и страхует от возможных ошибок подрядчика».

«При определенном бюджете и ресурсах взломать можно любую организацию, – заметил Сергей Левашов. – Наша задача – организовать инфраструктуру таким образом, чтобы злоумышленнику было максимально сложно это сделать. Во взаимоотношениях с подрядчиками контроль, я совершенно согласен, играет очень важную роль. Так, в одном крупном логистическом операторе, который был взломан, решили, что им проще потратить деньги на ликвидацию последствий, а не на реализацию мер защиты: «Поломают еще раз, еще раз восстановим. Бэкапы есть, все хорошо». Но их зарубежный партнер заявил, что если вы сейчас не защититесь должным образом, то мы вам регрессом выставим штрафные санкции по всем заключенным заранее договорам. Не знаю, имели ли они юридическое право так утверждать, но, тем не менее, угроза возымела действие, и компания начала защищаться. Подход «пусть ломают, но потом все исправим» порочен. А для объектов критической информационной инфраструктуры, тем более значимых, он незаконен. Даже с точки зрения коммерции ущерб может быть гораздо серьезнее, чем мы рассчитываем».

О деятельности Общественного совета при Министерстве транспорта Российской Федерации в области обеспечения информационной безопасности объектов транспортной инфраструктуры рассказал председатель Комиссии по вопросам транспортной безопасности и безопасности на транспорте Общественного совета при Минтрансе России **Вячеслав Керов**: «Совет тесно взаимодействует с ФГБУ «СИЦ Минтранса России», ФГУП «ЗащитаИнфоТранс», ФГУП ГосНИИ ГА. Работают комиссии по вопросам цифровой трансформации государственного управления на транспорте, транспортной безопасности и безопасности на транспорте. Транспортная безопасность – это защита от актов незаконного вмешательства. Она, конечно же, включает информационную безопасность, потому что любое оборудование имеет программное обеспечение. В рамках Комиссии по вопросам транспортной безопасности и безопасности на транспорте функционирует ряд рабочих групп. В их числе: рабочая группа по вопросам транспортной (авиационной) безопасности, куда



входят представители авиакомпаний и аэропортов, отвечающих за безопасность и информационную безопасность в частности, представители Ространснадзора и Росавиации; рабочая группа по мониторингу проблем, достижений и выполнения нормативно-правовых актов в области обеспечения транспортной безопасности транспортных средств и объектов транспортной инфраструктуры; рабочая группа по вопросам категорирования объектов критической информационной инфраструктуры, в которую входят представители Минтранса, ФГУП «ЗащитаИнфоТранс», ведущие интеграторы и вендоры».

Он отметил остро стоящий вопрос закупки нового оборудования для объектов транспортной инфраструктуры у дружественных стран на операционной системе Windows: «Часто слышим такое обоснование: это закрытый контур без подключения к интернету. Но если внимательно прочитать указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», то в нем нет понятий «закрытый контур», «открытый контур». В нем четко сказано, что в целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации программное обеспечение должно быть отечественным».

Также Вячеслав Керов коснулся вопроса категорирования объектов КИИ: «Еще в 2024 году Минтранс отправил письмо порядка 900 компаниям и организациям транспортной отрасли о необходимости категорирования. На сегодняшний день категорировалось 60% в лучшем случае. Наша профильная рабочая группа, которую возглавляет Сергей Половников, ведет активную работу в этом направлении – убеждаем проходить эту процедуру. Кстати, Министр транспорта Российской Федерации Андрей Никитин на встречах с первыми лицами субъектов РФ этот вопрос регулярно поднимал».

«Позвольте напомнить, закон действует с 1 января 2018 года, а мы всё еще говорим о категорировании, – обратилась к участникам пленарной сессии Елена Торбенко. – Категорирование, конечно, нужно, но для того, чтобы понять, что необходимо защищать, в какой степени и сколько денег на это тратить. Давайте говорить о реальной защите. Бывают такие ситуации, когда вы не можете закупить новое

оборудование либо внедрить отечественное ПО. Отечественные средства защиты не всегда «дружат» с прикладным программным обеспечением, и, чтобы провести испытания, нужны время и средства. Значит принимайте предписанные нами организационные меры для обеспечения безопасности. Все можно решить. План – это хорошо, но пора переходить к практике и фактической реализации мероприятий с помощью вашего регулятора».

«Здесь очень важно, как выстроено внутри компании взаимодействие ИТ-специалистов и специалистов по информационной безопасности, – сказал Сергей Левашов. – С моей точки зрения, исходя из полученного опыта, наличие двух руководителей по этим направлениям усложняет процесс. Единоначалие более эффективно – не возникает конфликта интересов. И, конечно, любой вопрос информационной безопасности, защиты информационных систем и периметра решается ИТ-средствами».

«Я согласна с вами, что нужно упрощать и говорить на вашем языке, но служба, которую я представляю, является межотраслевым регулятором. Пока что у нас под законом 14 сфер, и наши документы изданы так, чтобы они были применимы для всех 14 сфер, – прокомментировала Елена Торбенко просьбу об упрощении и уточнении требований ФСТЭК России. – В наших документах вы не увидите конкретной карты действий вроде «поставьте шесть галочек в таком-то средстве защиты». Если мы жестко загоним вас в рамки, вы просто не сможете жить: любой шаг в сторону будет считаться побегом. Но некие рекомендации с учетом отраслевых особенностей могут появиться, законом они предусмотрены».

«Действительно, такая работа ведется, – подтвердил Сергей Страхов. – На базе ФГУП «Защита-ИнфоТранс» образована экспертная группа, составленная из представителей ведущих предприятий и вендоров. В нее входят крупные отраслевики по каждому из направлений транспорта. В планах Минтранса до конца года отправить на согласование во ФСТЭК России верхнеуровневый документ, который бы определял перечень классов систем, с нашей точки зрения необходимых к использованию с определенной степенью типизации. Упоминания конкретных продуктов, безусловно, в нем не будет». ■

Александр Никитушин
Фото: Мария Мурашова



BPMSOFT | LANSOFT

Российская ИИ-платформа для управления административными процессами в транспортной отрасли

- **Ускоряйте** обработку обращений граждан и организаций
- **Автоматизируйте** согласование, поручения и контроль исполнения
- **Выстраивайте** межведомственное взаимодействие



Готовы обсудить цифровизацию вашей организации?

Сертифицирована ФСТЭК России по 4 уровню доверия

Входит в реестр российского программного обеспечения

Рекомендована для проектов импортозамещения на объектах КИИ

Соответствует требованиям 152-ФЗ «О персональных данных»

г. Москва, ул. Бутырская, д. 76с1

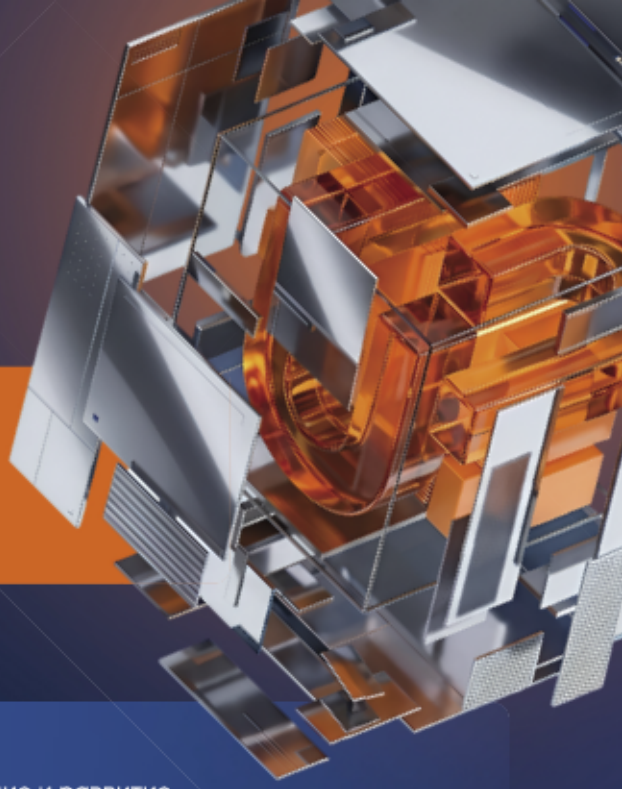
+7 (495) 070-09-97

info@bpmsoft.ru

Реклама ООО «БПМСофт» ИНН 7724744134

INNOSTAGE

ПРОВАЙДЕР КИБЕРУСТОЙЧИВОСТИ



Innostage обеспечивает цифровую устойчивость лидеров рынка, имеющих высочайшие требования к уровню информационной безопасности

КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ:

01 Информационная безопасность

02 Системная интеграция

03 Построение и развитие ИТ-инфраструктуры

04 Внедрение средств защиты информации

05 Разработка бизнес-решений и ПО

06 Консалтинг

07 Безопасность АСУ ТП

На базе Innostage функционирует профессиональный центр противодействия киберугрозам **Innostage SOC CyberART**, осуществляющий комплексный подход к противодействию цифровым угрозам. Является центром ГосСОПКА.

Innostage более шести лет успешно работает на российском рынке информационной безопасности и занимает лидерские позиции в отраслевых рейтингах.



1 МЕСТО

среди крупнейших отечественных поставщиков ИБ-сервисов

CNews Analytics

ТОП-8

крупнейших ИБ-компаний в России

Tadviser

ТОП-40

в рейтинге 500 крупнейших ИТ-компаний России 2024

CNews

innostage-group.ru

Telegram

МАКС

info@innostage-group.ru

+7 (843) 567-42-90

РЕКЛАМА

ФУНКЦИОНАЛЬНАЯ УСТОЙЧИВОСТЬ ТРАНСПОРТА: КАК СОХРАНИТЬ ПЕРЕВОЗКИ ПРИ ЦИФРОВЫХ СБОЯХ

Последствия цифровых сбоев на транспорте по масштабу и тяжести уже сопоставимы с физическим повреждением инфраструктуры. Защита периметра и резервирование систем, данных и каналов связи не гарантируют устойчивой работы критичных функций, таких как управление движением, оформление перевозок, досмотр и работа пунктов пропуска. Дмитрий Шепелявый, директор по развитию международного бизнеса Innostage, рассказывает, как обеспечить реальную непрерывность транспортных процессов при инцидентах информационной безопасности.



Дмитрий Шепелявый,
директор по развитию международного бизнеса Innostage

ПОЧЕМУ ЗАЩИТЫ ИТ-СИСТЕМ НЕДОСТАТОЧНО

Цифровые документы для перевозки, логистические платформы, пассажирские сервисы и беспилотные технологии стали составной частью цифрового контура транспортной отрасли. Их работа напрямую зависит от устойчивости информационных систем.

Обычно устойчивость обеспечивают через резервирование систем, данных и каналов связи. Однако целью кибератак все чаще становятся сами резервные копии, и такой подход уже не покрывает все аварийные сценарии. По данным Минтранса, только за первый квартал 2026 года зафиксировано более 9 тысяч кибератак на транспортную инфраструктуру РФ, что на 10% больше, чем за весь 2025 год. Мировая статистика показывает, что в 94% атак с помощью программ-вымогателей злоумышленники целенаправленно пытались повредить резервные копии, и в 57% случаев им это удалось. Когда резервные копии оказываются скомпрометированы, медианная стоимость восстановления вырастает примерно в восемь раз – с $375 тысяч до $3 миллионов.

Принято считать, что функциональная устойчивость транспорта – задача информационной безопасности. На деле функциональная устойчивость – более широкое понятие. Информационная безопасность – это одна из восьми ее составляющих наряду с архитектурой, непрерывностью, эксплуатацией, данными, персоналом, внешними зависимостями и доверенностью. Влияние внешних зависимостей упускают из виду чаще остальных. Функция внутри организации по документам может быть защищена и зарезервирована, но сбой платформы подрядчика или магистрального канала связи остановит важные процессы.

ЧТО ТАКОЕ ФУНКЦИОНАЛЬНАЯ УСТОЙЧИВОСТЬ

Функциональная устойчивость транспортного комплекса – это способность критичных функций сохранять доступность, производительность, целостность данных и время восстановления при любом негативном воздействии.

Работу по обеспечению функциональной устойчивости транспортного комплекса логично начинать с подготовки каталога критичных процессов

и реестра недопустимых событий. Например, в список включают: «недоступность услуги для значительного числа граждан», «остановку перевозочного процесса», «нарушение работы пункта пропуска», «подмену данных о грузе и маршруте» и т. п. Затем функции и события необходимо ранжировать по классам критичности: от непрерывно-критичных, где нарушение затрагивает безопасность движения или массовую доступность услуг, до поддерживающих.

Допустимое время простоя и допустимый объем потери данных для каждой критической функции определяет ее владелец – ответственный руководитель или подразделение. Он исходит из того, насколько долго функция может быть недоступна и какие данные можно потерять без существенного ущерба для работы транспорта. Требования к безопасности движения и транспортной безопасности дополнительно ужесточают ограничения для технологических систем: сбой или утрата данных не должны создавать рисков для перевозок, управления инфраструктурой и пассажиров.

Транспортная функция редко замкнута в одной организации: отказ общей платформы обмена данными или магистрального канала связи способен остановить работу сразу нескольких участников. Поэтому внешние зависимости нужно выявлять заранее и учитывать наравне с устойчивостью собственной инфраструктуры. В этом помогает карта зависимостей «функция – сервис – элемент – канал – поставщик – персонал»: она показывает узлы, сбой в которых затрагивает сразу несколько организаций и функций. Именно их в первую очередь нужно резервировать и разделять, чтобы отказ не распространялся на смежные процессы.

КАК ОБОСНОВАТЬ ИНВЕСТИЦИИ

Функциональной устойчивости сложно достичь без регулярного проведения тестов и учений. Каждая заявленная метрика – время восстановления, допустимая потеря данных или готовность персонала – должна быть подкреплена конкретным артефактом: время восстановления – протоколом теста, потеря данных – отчетом о точке восстановления и проверкой целостности копии, готовность персонала – отчетом об учении.

Комплексная методика проверок включает в себя три этапа: технический тест восстановления с фиксацией фактических параметров, функциональное учение с переходом на ручной или локальный режим и действия дежурной смены под сценарий недопустимого события.

Даже при наличии резервных копий и готовых к работе резервных систем учения выявляют проблемы: фактическое время восстановления оказывается в разы больше заявленного, резервная копия базы данных – неполной или поврежденной, переключение на резервные системы под нагрузкой ранее не отрабатывалось, а у персонала нет регламента перехода на ручной режим. Учения позволяют заблаговременно выявить и устранить эти расхождения до наступления негативных последствий.

Чтобы результаты проверок помогали принимать управленческие решения, вводится измеримый показатель. В его основе лежит интегральный индекс по шкале от 0 до 100, который рассчитывается с учетом оценок по отдельным доменам функциональной устойчивости: от доступности и восстановимости до доверенности. Индекс можно разворачивать до уровня конкретной функции, объекта и организации. Меры ранжируются по величине подтвержденного разрыва и по тому, насколько они снижают ожидаемые годовые потери. Самое слабое звено показывает реальный уровень функциональной устойчивости компании и определяет необходимые направления для инвестиций.

ПОЧЕМУ НУЖНА КООРДИНАЦИЯ РЕГУЛЯТОРА

Часть задач по обеспечению функциональной устойчивости решается внутри транспортной компании: это обоснование параметров критичных функций, построение наблюдаемости, проверка восстановимости и устранение разрывов, выявленных на учениях. Координацию внедрения можно поручить корпоративному Центру управления функциональной устойчивостью. Он собирает разрозненные сигналы от действующих диспетчерских и мониторинговых центров, не подменяя их работу, и может работать в связке с отраслевым центром, создаваемым Минтрансом.

Но есть задачи, которые силами отдельной компании не решаются. Отрасли нужны единый стандарт функциональной устойчивости, общий каталог критичных функций, реестр недопустимых событий и методика расчета индекса. Без общего языка и сопоставимых метрик нельзя сравнить устойчивость объектов, рассчитать отраслевую картину, скоординировать действия при сбое, затрагивающем нескольких участников. Здесь нужна помощь Минтранса как регулятора, который видит отрасль целиком и координирует организации и виды транспорта.

РЕКЛАМА

ТРЕНДЫ КИБЕРБЕЗОПАСНОСТИ – 2027: К ЧЕМУ ГОТОВИТЬСЯ ТРАНСПОРТНОЙ ОТРАСЛИ

Автоматизация логистики, развитие интеллектуальных транспортных систем (ИТС) и внедрение умных сервисов для пассажиров – неотъемлемые процессы эффективного развития транспортной отрасли. Однако оборотной стороной ускоренных темпов цифровизации становится рост уязвимости критических инфраструктур. О том, как защитить отрасль в эпоху гибридных угроз, рассказал Егор Куликов, руководитель направления безопасности КИИ и АСУ ТП в К2 Кибербезопасность.



Егор Куликов,
руководитель направления безопасности КИИ и АСУ ТП в К2 Кибербезопасность

ТРИ ГЛАВНЫХ ВЫЗОВА ТРАНСПОРТНОЙ ОТРАСЛИ

– Егор, какие ИБ-вызовы стоят перед индустрией сегодня?

– Можно выделить три ключевых вызова. Первый – беспрецедентное увеличение киберугроз и их усложнение. При этом атаки становятся все целенаправленнее. Для транспорта это особенно критично, так как остановки процессов влияют на большое количество людей и могут иметь самые разные по масштабу последствия: злоумышленники могут скомпрометировать системы управления воздушным движением, изменить планы полетов в аэропортах, взломать диспетчерские центры железных дорог, подменив сигналы блокировок на путях и полностью парализовав движение поездов.

Второй вызов – продолжающийся кадровый голод. Отраслевые системы имеют свою специфику, а безопасников с такой экспертизой сильно не хватает.

Третий вызов – особые требования ИБ-законодательства. По ФЗ № 187 транспортные организации, как субъекты КИИ, обязаны категорировать свои ИТ-системы, обеспечивать их непрерывную защиту сертифицированным отечественным софтом и передавать данные об инцидентах в ГосСОПКА. Также по Указу Президента № 250 все субъекты КИИ уже давно должны были полностью отказаться от ИТ- и ИБ-продуктов вендоров из «недружественных» стран.

– Насколько успешно идет импортозамещение?

– Согласно нашим опросам рынка, импортозамещение все еще продолжается, так как это крайне ресурсозатратный процесс. Основные причины: дефицит бюджетов, сжатые сроки и общая неготовность ИТ-инфраструктур к изменениям. К тому же из-за отсутствия профильных специалистов транспортным компаниям трудно самостоятельно ориентироваться в измененной карте рынка отечественных ИБ-решений. В итоге мы часто видим кейсы с неверным выбором или некачественной настройкой средств защиты, что ведет к лишним расходам.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ, ИТ И ИБ – БАЗОВАЯ СВЯЗКА В ТЕКУЩИХ РЕАЛИЯХ

– В последнее время эксперты все чаще говорят о слиянии информационной и физической безопасности. Что стало триггером этого процесса?

– Темпы развития технологий. Системы видеонаблюдения, досмотровые комплексы и т. д. перестали быть изолированными аналоговыми контурами. Оборудование на вокзалах и в терминалах сегодня само генерирует метаданные и интегрируется в ИТ-сеть. Как только физическое устройство получает IP-адрес, грань между физической охраной и ИБ исчезает – камера становится частью ИТ-инфраструктуры, которую нужно защищать от программных атак. Уязвимости на стыке физического доступа и цифровой среды часто становятся первоначальной точкой входа для злоумышленников. Для большинства компаний ИБ и служба физической охраны (СБ) – это два разных мира. Этот разрыв очень опасен, так как порождает размытие зон ответственности.

Теперь эффективность физической защиты и кибербезопасности зависит от того, насколько они интегрированы между собой. Спрос на такие услуги активно растет. И в этом году мы вместе с коллегами из «К2Тех» выделили отдельную команду под комплексные проекты по защите физических и цифровых инфраструктур, куда входят: кибербезопасность, защита периметра, умный противопожарный комплекс и любые необходимые виды работ. Это подход «единого окна»: аудит, разработка стратегии и дорожной карты, проектирование, строительно-монтажные и пусконаладочные работы, внедрение и настройка необходимых средств защиты, круглосуточный мониторинг и техническое обслуживание.

– ***Каким вы видите эффективное взаимодействие ИТ и ИБ?***

– ИТ и ИБ должны работать в тесной связке. Мы здесь опять говорим об ускоренной автоматизации самых разных процессов. А любая цифровизация должна сразу сопровождаться продуманной стратегией по кибербезопасности. Иначе рано или поздно вы столкнетесь с негативными последствиями для всего бизнеса: шифрованием данных, остановкой процессов, утечкой данных клиентов и партнеров и т. д. ИТ-инфраструктура должна быть сразу готова к интеграции средств защиты.

Не так давно к ИБ-рискам также добавился искусственный интеллект, а точнее разрыв между его повсеместным внедрением и умением делать это безопасно. Каждую неделю растет количество инцидентов с негативными последствиями от использования ИИ-моделей. Согласно результатам нашего исследования с «Лабораторией Касперского», 38% корпораций уже занимаются разработкой собственных ИИ-решений для внутренних процессов. При этом 75% из них не умеют делать их безопасными для бизнеса. Зрелый подход – сразу встраивать этот новый класс рисков в систему своего стратегического планирования. А это невозможно без налаженной и доверительной коммуникации между ИТ и ИБ.

ЧТО ДЕЛАТЬ?

– ***Как минимизировать риски киберугроз в текущих условиях?***

С учетом растущего уровня киберугроз рынок перестраивается и смотрит в сторону более масштабных систем защиты. А именно – SOC (Центры мониторинга кибербезопасности), которые включают в себя три базовых элемента: регулярно обновляемый технологический стек, профессиональную ИБ-команду и налаженные процессы по выявлению инцидентов и реагированию на них.

Важно понимать, что эпоха, когда было достаточно просто установить решение из коробки, давно прошла. Сегодня кибербезопасность – это про комплексность: подготовленная и правильным образом настроенная ИТ-инфраструктура, средства защиты, круглосуточный мониторинг и реагирование на инциденты, команда опытных специалистов и налаженные процессы, когда все понимают свои зоны ответственности. Важно понимать, что кибербезопасность – это никогда не прекращающийся процесс. Подходы должны постоянно пересматриваться, а решения регулярно обновляться. Также необходимы регулярные испытания инфраструктуры на киберустойчивость (пентесты, проверка работы команды защитников и др.), которые определяют текущий уровень защиты и точки роста для нового апгрейда.

О КОМПАНИИ:

К2 Кибербезопасность (входит в К2Тех) – бизнес-партнер по выстраиванию практической кибербезопасности, в частности КИИ и АСУ ТП: от проектирования ИБ-систем с нуля до построения передовых концепций киберзащиты с мониторингом и технической поддержкой 24/7.

РЕКЛАМА

ЦИФРОВИЗАЦИЯ ТРАНСПОРТА: СИСТЕМ БОЛЬШЕ, А УПРАВЛЕНИЯ МЕНЬШЕ?

Почему безопасность транспорта зависит не только от защиты информации, но и от постоянного развития цифровых систем.



Артем Зотов, *генеральный директор компании «Транснависофт»*

В предыдущей статье мы говорили о том, что безопасность информационной системы определяется не местом размещения сервера, а тем, кто отвечает за ее работу, обновление и защиту.

Но сегодня возникает другая проблема. Информационных систем становится больше, интеграций между ними – еще больше, а внимания к сопровождению уже внедренных решений зачастую становится меньше.

Регионы активно внедряют мониторинговые системы, аналитические платформы, решения для учета пассажиропотока и контроля транспортной работы. Мы научились собирать огромное количество информации. Но научились ли мы лучше управлять транспортом?

МНОГО СИСТЕМ. А КТО УПРАВЛЯЕТ?

Мониторинговая система показывает, где находится автобус. Аналитическая объясняет, что происходило вчера. Контрольная фиксирует нарушения. Но кто должен влиять на перевозочный процесс сегодня, пока автобус еще находится на линии?

Эту задачу решает диспетчерская система. Именно она связывает расписание, выпуск транспорта, выполнение рейсов, соблюдение интервалов и диспетчерские воздействия. По сути, диспетчерская система должна становиться центром накопления, проверки и оптимизации транспортных данных. Она объединяет информацию о маршрутах, перевозчиках, транспортных средствах, пассажиропотоке и фактически выполненной работе, превращая ее в управленческие решения.

Однако во многих проектах внимание сосредоточено на создании новых аналитических инструментов, тогда как сами диспетчерские системы продолжают работать на прежней архитектуре, с накопленными доработками и устаревающими интеграциями.

Получается интересная ситуация. Мы совершенствуем инструменты наблюдения, но забываем развивать инструменты управления. Можно установить в диспетчерской двадцать экранов вместо пяти. Но разве от этого автобус, выбившийся из расписания, самостоятельно вернется в график?

ДАННЫЕ ЕСТЬ. А МОЖНО ЛИ ИМ ВЕРИТЬ?

Любой инженер знает, что измерительные приборы необходимо периодически проверять и калибровать. Возьмем датчик пассажиропотока. При становке он показывает корректные значения. Но со временем загрязняется оптика, меняются условия эксплуатации, сбиваются настройки. Данные продолжают поступать. Отчеты формируются. Графики выглядят убедительно. Но кто проверяет, насколько эти цифры соответствуют действительности? Ни одна аналитическая платформа не исправит недостоверные исходные данные исключительно за счет красивых графиков.

С программным обеспечением происходит то же самое. Меняются маршруты, справочники, алгоритмы расчетов, законодательство и протоколы обмена данными. При этом система может продолжать работать без видимых сбоев. Но означает ли это, что она по-прежнему работает правильно?

ДАЖЕ АВТОМОБИЛЮ В ГАРАЖЕ НУЖНО ТЕХОБСЛУЖИВАНИЕ

Представим, что вы купили автомобиль и поставили его в гараж на год. Пробег не увеличился, аварий не было. Казалось бы, зачем техническое обслуживание? Но жидкости стареют, резиновые элементы теряют свойства, аккумулятор разряжается. Даже автомобиль, который никуда не ездит, требует внимания.

Почему же к информационным системам мы относимся иначе? Программа, установленная пять лет назад, может исправно запускаться. Но за это время изменились операционные системы, требования безопасности, внешние сервисы и нормативная база.

А теперь представим, что к автомобилю постоянно подключают новые датчики, камеры и экраны, но двигатель принципиально не обслуживают. Не напоминает ли это современную цифровизацию транспорта?

Причем с информационными системами ситуация опаснее. Неисправный автомобиль рано или поздно остановится. А устаревшая программа может годами выдавать некорректные результаты, оставаясь формально работоспособной.

ИНТЕГРАЦИЯ ЕЩЕ НЕ ОЗНАЧАЕТ ЕДИНУЮ СИСТЕМУ

Сегодня практически каждый новый транспортный ИТ-проект предусматривает интеграции. Но что именно мы интегрируем? Одна система считает рейс по расписанию, другая – по навигационным событиям, третья – по собственным алгоритмам. В результате один и тот же автобус может выполнить разное количество рейсов в разных отчетах. И каждый разработчик скажет, что его система работает корректно. Так кто же прав?

Проблема заключается не только в программном обеспечении, но и в отсутствии единых правил формирования данных. Поэтому транспортной отрасли необходимы общая нормативно-справочная информация, согласованные модели данных и диспетчерская система, которая связывает все вокруг реального перевозочного процесса. Иначе мы рискуем получить десятки информационных систем, каждая из которых знает свою правду.

SAAS – ЭТО НЕ ТОЛЬКО ОБЛАКО

Именно здесь мы возвращаемся к вопросу SaaS и локального лицензирования. Главное преимущество правильно организованной сервисной модели заключается в том, что развитие программного обеспечения становится частью его ежедневной эксплуатации.

Изменилось законодательство? Появилась новая интеграция? Обнаружена уязвимость? Требуется изменить алгоритм расчета рейсов? Поставщик может централизованно обновлять продукт, проверять изменения и поддерживать единую актуальную версию. При локальном размещении это тоже возможно, но требует отдельно организованного сопровождения, финансирования и своевременного внедрения обновлений.

И что происходит, когда на все это перестают выделять ресурсы? Ничего заметного. Система продолжает работать. Только ее соответствие реальному перевозочному процессу постепенно снижается.

Безусловно, SaaS сам по себе не гарантирует ни безопасности, ни достоверности данных. Но при правильно выстроенной архитектуре и договорной ответственности он позволяет сделать сопровождение и развитие системы непрерывным процессом, а не очередным проектом модернизации.

НЕ НАБЛЮДАТЬ, А УПРАВЛЯТЬ

На мой взгляд, нам пора перестать измерять уровень цифровизации количеством внедренных систем. Гораздо важнее задавать другие вопросы. Можно ли доверять данным? Можно ли сопоставить конкретный рейс с пассажиропотоком, оплатой проезда и выполненной транспортной работой? Может ли диспетчер не только увидеть нарушение, но и повлиять на ситуацию? Кто отвечает за актуальность алгоритмов и интеграций? И главное, будет ли вся эта инфраструктура столь же надежно работать через три года?

Мы не должны прийти к ситуации, когда регион прекрасно знает, почему транспорт работает плохо, но не располагает инструментами, чтобы заставить его работать лучше.

Цифровизация должна развиваться от наблюдения к управлению, от разрозненных интеграций к единой архитектуре, от покупки программного обеспечения к непрерывному сопровождению.

Ведь безопасность транспорта – это не только защита данных от внешних угроз. Это уверенность в том, что данные достоверны, алгоритмы актуальны, а решения принимаются на основании реального положения дел.

И если автомобиль без технического обслуживания рано или поздно перестанет ехать, то информационная система без сопровождения может продолжать работать годами. Только вот правильно ли она работает – об этом мы можем даже не узнать.

НА III ВСЕРОССИЙСКОМ ФОРУМЕ «ТРАНСПОРТНАЯ РЕФОРМА» В КРАСНОЙ ПОЛЯНЕ ОБСУДИЛИ БУДУЩЕЕ ОТРАСЛИ

Мероприятие объединило представителей 35 регионов России. В центре внимания оказались цифровизация пассажирских перевозок, развитие единой билетной системы, внедрение биометрических технологий и новые цифровые сервисы. Одним из ключевых итогов стало подписание соглашения о запуске московской билетной системы в Северной Осетии.

С 30 сентября по 2 октября в Красной Поляне прошел форум «Транспортная реформа: новые возможности», организованный компанией «СберТройка» при поддержке Департамента транспорта и развития дорожно-транспортной инфраструктуры Москвы и Сбера. Мероприятие собрало более 180 представителей органов власти, транспортных операторов, технологических компаний и отраслевых экспертов.

За три года форум стал значимой отраслевой площадкой для обмена опытом и поиска практических решений. Особое внимание уделяется технологиям, которые помогают регионам модернизировать транспортную инфраструктуру, повышать эффективность управления перевозками и делать поездки комфортнее для пассажиров.

«Мы создавали этот форум как пространство для открытого диалога и обмена практическим опытом. Для нас важно, чтобы регионы могли напрямую делиться своими достижениями, успешными кейсами и результатами внедрения новых технологий с нашими заказчиками, партнерами и коллегами по отрасли. У каждого региона есть уникальный опыт и решения, которые могут быть полезны другим. Наша задача – объединить эти знания, создать условия для профессионального взаимодействия и помочь успешным практикам находить применение по всей стране», – отметила генеральный директор ООО «СберТройка» **Елена Колесникова**.



Елена Колесникова,
генеральный директор ООО «СберТройка»

ЕДИНОЕ БИЛЕТНОЕ ПРОСТРАНСТВО: ТЕХНОЛОГИИ ДЛЯ РЕГИОНОВ

Деловую программу форума открыла закрытая сессия Общественного совета при Министерстве транспорта Российской Федерации, посвященная развитию платформенной экономики и цифровизации пассажирских перевозок. Модератором выступил Алексей Зотов, председатель профильной комиссии Общественного совета при Минтрансе России.

Участники обсудили интеграцию цифровых решений в единую транспортную экосистему, отраслевые барьеры и потребности регионов в новых технологических инструментах. Особую активность в дискуссии проявили представители Ростовской, Новосибирской, Пензенской областей, Санкт-Петербурга и других субъектов РФ, поделившиеся опытом и актуальными запросами.

«На форуме прошла очень важная для нас сессия. Мы собрали представителей регионов и постарались посмотреть на цифровизацию транспорта не через отдельные продукты и системы, а через то, как все это работает в едином контуре. Регионы очень предметно рассказали, что уже внедрено, где сегодня не хватает связности между системами и каких решений они ждут на федеральном уровне. Для нас теперь важно систематизировать эти запросы, выделить лучшие

практики и продолжить их проработку уже на площадке Общественного совета при Минтрансе России», – отметил председатель Комиссии по вопросам развития пассажирских перевозок Общественного совета при Минтрансе России **Алексей Зотов**.

На стратегической сессии «СберТройки» эксперты представили результаты запусков московской билетной системы в субъектах РФ и обсудили расширение ее географии. Отдельное внимание уделили карте «Тройка» как универсальному инструменту оплаты проезда, развитию безналичных расчетов и технологическим решениям для межрегиональных перевозок.

Московская билетная система уже зарекомендовала себя как масштабируемое решение, которое можно адаптировать под особенности транспортной инфраструктуры разных территорий. Для пассажиров это означает появление привычных способов оплаты, а для региональных властей – дополнительные инструменты анализа поездок и управления маршрутной сетью.

Одним из практических результатов форума стало подписание соглашения между Правительством Москвы, компанией «СберТройка» и властями Республики Северная Осетия – Алания о запуске московской билетной системы на базе карты «Тройка» в регионе.

В рамках деловой программы эксперты также обсудили развитие цифровых сервисов, призванных сделать повседневные поездки удобнее для пассажиров. В частности, «СберТройка» представила решение для льготных категорий граждан, предусматривающее интеграцию билетной системы с мессенджером MAX. Новые возможности позволят упростить подтверждение права на льготный проезд и сделать использование транспортных услуг доступнее.

Отдельное внимание уделили цифровизации автовокзалов и межрегиональных перевозок. «СберТройка» представила комплексный продукт для автоматизации работы автовокзалов, объединяющий в единой системе ключевые операционные процессы: от формирования и актуализации расписания рейсов до организации безналичных расчетов с перевозчиками. Решение также предусматривает автоматическое обновление информации на электронных табло и управление аудиооповещениями, позволяя оперативно информировать пассажиров об отправлении, прибытии и изменениях в движении автобусов. Такой подход помогает сократить объем ручных операций, повысить прозрачность финансовых расчетов и обеспечить согласованную работу всех участников перевозочного процесса.



Еще одним примером цифровизации пассажирских перевозок стал проект «Суда сюда!» компании «СберТройка». Он объединяет сервисы оплаты проезда на борту судов и в кассах на причалах. На сайте пассажиры могут выбрать подходящий маршрут, ознакомиться с расписанием и узнать стоимость поездки.

Продолжением обсуждения стала межрегиональная дискуссия, посвященная внедрению транспортных решений Правительства Москвы. Представители регионов обменялись опытом применения технологий, которые уже доказали свою эффективность в столице, и обсудили возможности их адаптации к особенностям местных транспортных систем.

«Для нас важно, что форум «Транспортная реформа» приносит практические результаты. Регионы не только обмениваются опытом и знакомятся с новыми технологиями, но и выбирают решения, которые помогают повышать качество пассажирских перевозок. Так, по итогам форума 2025 года к билетной системе «СберТройки» присоединились еще четыре региона России. Третий год подряд мы видим интерес регионов к участию в мероприятии и намерены продолжать эту работу», – подчеркнула генеральный директор ООО «СберТройка» **Елена Колесникова**.

СПРАВКА О ФОРУМЕ

Всероссийский форум «Транспортная реформа: новые возможности» проводится с 2024 года. Организатором выступает компания «СберТройка» при поддержке Департамента транспорта и развития дорожно-транспортной инфраструктуры Москвы и Сбера.

Форум создан как площадка для обмена опытом, объединения отраслевой экспертизы и тиражирования успешных практик на стыке финансовых технологий, ИТ и транспортных услуг. Мероприятие способствует развитию профессионального диалога между представителями власти, бизнеса и технологических компаний, а также внедрению современных решений в транспортные системы регионов России.

РЕКЛАМА

«СТУДЕНЧЕСКИЙ» АЭРОПОРТ: КАК МОЛОДОСТЬ ВЛИЯЕТ НА ТРАНСПОРТНУЮ БЕЗОПАСНОСТЬ

Транспортная отрасль России связывает нашу страну в единый организм. На транспорте трудится более 4 миллионов человек, и исторически студенческие отряды всегда привлекались как к строительству транспортной инфраструктуры, так и к ее обслуживанию. Это и БАМ, и дорожные магистрали, и, конечно, работа проводниками. Но сегодня я хочу заострить внимание на проекте, реализуемом в аэропорту Пулково, который дает новое дыхание РСО, – всероссийском сводном студенческом сервисном отряде «Взлетная полоса».



Алексей Потейко,
председатель Комиссии по вопросам проведения молодежной политики в сфере транспорта Общественного совета при Минтрансе России, заместитель председателя Наблюдательного совета Российских студенческих отрядов

Для меня как члена Общественного совета при Минтрансе России принципиально важно, что мы выходим на углубленное взаимодействие с Росавиацией. И здесь есть знаковый организационный сдвиг: в Общественный совет при Росавиации вошла представитель Российских студенческих отрядов **Екатерина Грязнова** – руководитель направления студенческих сервисных отрядов Центрального штаба РСО. Это сигнал: отрасль заинтересована тиражировать наш опыт, донося его всем субъектам авиаперевозок.

Почему это принципиально?

Потому что транспортная безопасность для нашей страны – вопрос функционирования и выживания всей системы. И особенно остро это проявилось в последние годы. Массовые сбои в системе аэропортового обслуживания пассажиров стали не редкостью. Большинство этих сбоев было вызвано террористическими атаками украинских боевиков, но глубинные причины во многом связаны с недостатком персонала в различных службах аэропортов. Эксперты прямо связывают тревожные тенденции в наземном обслуживании аэропортовой инфраструктуры с острым дефицитом кадров.

Кадровая проблема в Пулково, втором аэропорту страны по объему перевозок, решилась после привлечения студенческих отрядов, это сгладило остроту вопросов пиковых перегрузок.

Когда я рассказываю об этом, эксперты отрасли часто спрашивают: «Какая безопасность может быть обеспечена с привлечением неопытных молодых сотрудников?» Если не погружаться в системный подход Пулково и РСО, в такой постановке вопроса, наверное, есть доля истины. Однако, если посмотреть на те службы, куда привлечены студенческие отряды (а их сегодня в аэропорту уже шесть), преимущества, в том числе и касающиеся безопасности, налицо:





- **Надежный (чистый) контингент.** Сегодняшняя система образования создает определенные стандарты и воспитывает среду, когда в вузах учатся ребята, которые в подавляющем большинстве – добропорядочные люди. В этой категории девиантное поведение практически не встречается, чего нельзя сказать о временном персонале, который заполонил службы других аэропортов. Простой показатель: из 400 студентов РСО, направленных в службу безопасности для проверки, отказ получен только по 0,5%. В других категориях он может достигать 70% и более.
- **Мобилизационный ресурс в пиковые моменты.** При необходимости в срочном наборе персонала именно студенческий отряд позволяет быстро закрывать потребности в дополнительных кадрах. А ведь если что-то в аэропорту «западает», это может привести к общему коллапсу системы.
- **Обучаемость.** Именно категория «студенты» максимально быстро обучается и готова менять свои компетенции по нескольку раз за период работы. Способность этой категории учиться не сравнима ни с одной другой. При грамотном наставничестве это дает возможность быстро готовить востребованных сотрудников, которые могут безболезненно переходить из службы в службу.
- **Коммуникабельность.** Именно эта категория наиболее коммуникабельна с пассажирами, создает позитивное впечатление от аэропорта и снижает вероятность возникновения конфликтов, что тоже важно для безопасности.
- **Состояние здоровья**. Молодые люди реже болеют, более выносливы, за счет чего трудоспособнее других.
- И как бы это ни было странно, во многом благодаря уже длительному сроку работы отрядов в Пулково, программам профобучения РСО и наставничеству Пулково эта категория во многих профессиях **более компетентна и профессиональна.**



Опыт Пулково сегодня перенимают и другие аэропорты: Храброво, Внуково, Казань, Сочи и более мелкие, такие как Омск. Проект «Взлетная полоса» стартовал в 2021 году, и за это время к нему присоединились более 3000 ребят. Студенты могут выбрать одну из 25 профессий, а за время работы отработали более 1 миллиона часов. Более 200 участников выбрали Пулково для постоянной работы. В 2025 году здесь было задействовано более 600 бойцов РСО, а всего – около тысячи человек. В 2026 году проект вышел на международный уровень: 300 участников, из них 50 студентов из Белоруссии, Кыргызстана и Казахстана отработали в Пулково летом.

Но самое главное – это взгляд генерального директора компании «Воздушные Ворота Северной Столицы» **Леонида Сергеева**. Приведу его слова: «Мы являемся первым «студенческим» аэропортом. У нас до нынешнего года работало 1000 студентов. Но в этом сезоне мы делаем просто мегапрорыв. Мы увеличиваем эту

цифру до 2500. Получается, что к 3700 сотрудникам постоянного штата добавляется 2500 студентов со всех необъятных концов нашей Родины и стран СНГ. Это абсолютно другой эмоциональный фон, когда в аэропорту работает молодежь со всей страны. РСО под эти задачи подошли идеально, потому что студенческие отряды есть практически в каждом городе. К нам с 2023 года, когда мы начали сотрудничать, приезжают ребята из более чем 20 разных регионов. Мы разрешаем им работать в своей национальной одежде и использовать привычные им формы проявления внимания. Я сам с Урала – у нас свои традиции, в Уфе свои традиции, на Камчатке свои. И это просто супер. Мы смотрим на реакцию, обратную связь от пассажиров, и это фантастика!»

Это очень классно, и данный проект можно тиражировать на главные авиагавани страны. Пулково – первый «студенческий» аэропорт в России, сотрудничающий с 85 вузами и ссузами. И отрасль уже смотрит шире: в ближайшие пять лет мы планируем развернуть работу практически во всех крупных воздушных гаванях страны – не только в сервисе, но и в отрядах бортпроводников, а также в техническом составе авиации.



Это **высокий уровень оплаты труда,** а значит, и конкуренция среди отрядов за право участвовать в проекте.

Это **новые условия работы в круглогодичном формате для РСО**, что максимально интересно как кейс для других работодателей.

«Когда мы формируем состав студенческих отрядов для работы в Пулково, для нас важно, чтобы каждый понимал: безопасность – это не формальность на входе, а умение не растеряться, когда ситуация выходит за рамки привычного формата. Нам важно, чтобы каждый боец был готов к нестандартным ситуациям, ЧП и ЧС. Безопасность пассажиров начинается с системной подготовки отряда: с обучения и ответственности каждого на своем рабочем месте. И студенческие отряды к этому готовы!

Екатерина Грязнова, руководитель направления студенческих сервисных отрядов Центрального штаба МООО «РСО», член Общественного совета при Росавиации



Что такое студотрядовский аэропорт?

Это **лицо РСО**. Как и проводники, наши отряды в контакте с миллионами пассажиров. По итогам 2025 года годовой пассажиропоток аэропорта Пулково составил более 20,9 млн человек. Наши ребята на работе – лучшая реклама РСО.

Это **интересные профессии**, которые могут расширить пул образовательных организаций, заинтересованных в «профильности» отрядов, формируемых для аэропорта.

Ну и, конечно, это огромная **государственная задача – обеспечение конституционного права россиян на беспрепятственное перемещение.**

Все это круто и важно. Дополнительно я бы отметил, что для компаний транспортной отрасли это прецедент. Именно аэропорт Пулково более понятен средним предприятиям транспорта. Наша презентация опыта взаимодействия с ОАО «РЖД» у таких компаний не вызывает интереса, мы постоянно слышим: «Ну это же РЖД – у них все по-другому». И сегодня проект, который

развернулся в Пулково, дает нам новые возможности для тиражирования этого опыта как на другие аэропорты, так и на другие транспортные компании.

Как член Общественного совета при Минтрансе России я готов этому способствовать. И уверен, что в ближайшее время мы услышим об отрядах в крупнейших морских и речных портах России и на судах пассажирского и грузового флота. Кстати, первые ласточки уже есть – это отряды туристической инфраструктуры речных круизов. ПАО «Московское речное пароходство» много лет формирует сводный сервисный отряд из более чем 200 бойцов по таким профессиям, как горничная, официант, помощник повара, повар, кухонный работник, администратор, менеджер, бармен, аниматор, диджей. И да, на речном флоте навигация ограничена, но с мая по октябрь мы на борту!

В отрасли авиаперевозок эффект будет виден уже следующим летом. Пожелаем достичь в Пулково требуемого показателя, решив самый сложный вопрос обеспечения круглогодичного бесперебойного процесса работы отрядов в аэропорту. И конечно, эта молодежная сила помогает обеспечивать и транспортную безопасность: ребята – там, где нужны, они заряжены на результат, они гордятся своей работой, а коллективная – отрядная – ответственность мотивирует их работать лучше с каждым днем.





Фото: Российские студенческие отряды



ОТВЕТСТВЕННОСТЬ СЛЕДУЕТ ЗА ГРУЗОМ

Как создать сквозную систему страховой защиты логистической цепочки.



Сергей Бураго,
председатель Комиссии по вопросам развития грузовой логистики Общественного совета при Минтрансе России, президент Ассоциации участников внешнеэкономической деятельности в сфере таможенно-логистических услуг по содействию в развитии бизнеса

ОБЩЕСТВЕННЫЙ СОВЕТ
ПРИ МИНИСТЕРСТВЕ ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

Груз редко перемещается от отправителя к получателю силами одной компании. В цепочке поставок участвуют экспедитор, перевозчики, склады, терминалы и другие подрядчики. Груз принимают, передают, перегружают и временно хранят, при этом финансовая защита остается набором отдельных договоров. После утраты товара клиенту приходится выяснять, кто отвечал за него в конкретный момент.

Страхование груза и ответственности участников перевозки решает разные задачи. Полис на груз защищает интерес владельца. Страхование ответственности перевозчика или экспедитора действует, когда имеются основания для их ответственности. Выплата зависит от законодательных норм, условий договора и установленного лимита.

Клиент нередко воспринимает полис ответственности как гарантию возмещения полной стоимости отправки. Между тем стоимость груза может превышать лимит, а покрытие исключать военные риски, мошенничество, нарушение температурного режима, простой или передачу товара непроверенному подрядчику. Даже действующий полис не всегда означает достаточную защиту.

По данным Центробанка России, в 2025 году взносы по страхованию грузов уменьшились на 6,1%, до 49,2 млрд руб., тогда как общий грузооборот снизился лишь на 0,7%. Количество договоров сократилось заметнее объема премий, а средняя стоимость полиса выросла. Такая динамика может отражать экономию на страховании. Компании увеличивают франшизы, ограничивают набор рисков и оставляют полное покрытие, прежде всего для дорогих или сложных отправок. Для рынка это тревожный сигнал. Стоимость и протяженность маршрутов растут, а финансовая защита становится более избирательной.

Главная уязвимость появляется на стыке операций. Для бизнеса доставка через терминал с перегрузкой на поезд или судно остается одной поставкой, однако с правовой и страховой точки зрения это разные операции и разная ответственность. Если маршрут, хранение или подрядчики описаны неточно, часть пути может оказаться вне страхового покрытия.

Особенно сложно установить ответственность при переадресации, подмене перевозчика, использовании чужих документов или взломе учетной записи диспетчера. Страховщик может оценить событие как передачу товара неуполномоченному лицу, поэтому важны условия полиса, соблюдение процедур проверки контрагента, автомобиля, водителя, адреса доставки.

Проблема возможна и после прибытия груза. Если грузополучатель не осмотрел товар, не зафиксировал повреждение и подписал документ без замечаний, доказать обстоятельства убытка труднее. Де-юре перевозка завершена, ответственность всех участников перевозки исполнена, а грузополучателю остается вести долгие переговоры со страховой компанией. Поэтому ответственность отправителя, склада, терминала и получателя также должны входить в систему управления рисками.

С 1 марта 2026 года на платформе «ГосЛог» действует реестр уведомлений о транспортно-экспедиционной деятельности. Среди размещаемых сведений предусмотрена максимальная страховая сумма по договору ответственности экспедитора, если такой договор есть. Однако эта сумма не является обязательной финансовой гарантией и не подтверждает соответствие полиса конкретной перевозке.

С 1 сентября 2026 года основные перевозочные и экспедиторские документы по общему правилу оформляются онлайн и передаются в ГИС ЭПД. В цифровой контур ГИС ЭПД вошли накладные разных видов транспорта, заказы и заявки, поручение экспедитору, экспедиторская и складская расписки. Это позволяет точнее фиксировать участников, операции и юридически значимые действия. Но электронный документ не создает страховой защиты. ГИС ЭПД фиксирует только титулы – кто принял груз, кто передал и когда, – но не содержит страховых параметров. Требуется проверять действительность полиса, лимит, территорию, риски и соответствие конкретной отправке. Следующий этап развития платформы ГИС ЭПД должен связать сведения о перевозке с данными страховщиков и проверять покрытие до передачи груза.

Основой новой модели может стать принцип непрерывности. В каждый момент должен быть определен участник, под контролем которого находится груз, границы его ответственности и финансовое обеспечение возможного ущерба. Ответственность не должна размываться между договорами и подрядчиками.

Грузоотправитель должен отвечать за сведения о грузе, его упаковке и специальных условиях хранения/перевозки. Экспедитор должен отвечать за организацию перевозки, выбор подрядчиков и перевозочные документы. Перевозчик – за сохранность принятого груза, а склад и терминал – за хранение, обработку, перегрузку. Грузополучатель же должен вовремя принять и осмотреть груз, при наличии зафиксировать недостачу или повреждение и обязательно подписать закрывающие документы.

Эта схема не означает одинаковых требований ко всем участникам. Объем ответственности должен соответствовать той части риска, которой каждый участник перевозки реально управляет. Но для профессиональных участников, принимающих груз под свой контроль, ответственность необходимо подкрепить финансовым обеспечением.

Если применять обязательное страхование, то это, конечно, увеличит стоимость перевозок, и для низкорисковых перевозок такое повышение будет критично.

Более гибким решением здесь может стать финансовая гарантия ответственности экспедиторов, перевозчиков, складов и терминалов. Ее формой могут быть страховой полис, банковская гарантия, участие в обществе взаимного страхования или компенсационном фонде.

Размер обеспечения финансовой гарантии должен учитывать масштаб и риск деятельности (оборот, максимальная стоимость перевозимого груза, виды операций, география, история претензий). Добросовестная компания с проверенными подрядчиками и низкой убыточностью должна получать более выгодные условия страхования.

Финансовая гарантия и страхование груза выполняют разные функции и образуют два самостоятельных уровня защиты: первая обеспечивает ответственность профессионального участника логистической цепочки, второе защищает имущественный интерес владельца товара, что особенно важно при перевозке дорогих, опасных, скоропортящихся и иных высокорисковых грузов.

До начала перевозки цифровая платформа должна проверять статус участника и наличие обеспечения, сопоставлять параметры груза и маршрут с условиями покрытия. Электронный документ фиксирует каждую приемку и передачу. При страховом случае единая хронология покажет, в чьей зоне ответственности находился в этот момент времени груз и в пределах какого обеспечения следует предъявлять требование.

Для реализации предлагаемой модели необходимо установить единые требования к страховым данным, обеспечить проверку финансовых гарантий участников рынка через платформу «ГосЛог» и привязку страхового покрытия к конкретной перевозке посредством ГИС ЭПД.

Российскому рынку нужна сквозная система, в которой на всем пути следования груза можно установить ответственное лицо, проверить достаточность финансового обеспечения и быстро получить возмещение. ■

РЕКЛАМА

ПРОТИВОДЕЙСТВИЕ БПЛА В СФЕРЕ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

ОТ ОЦЕНКИ УЯЗВИМОСТИ ДО ПРЕСЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ: НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ И ПРОБЛЕМНЫЕ ВОПРОСЫ



Константин Белоусов, *руководитель рабочей группы по вопросам совершенствования деятельности ПТБ Комиссии Общественного совета при Минтрансе России, генеральный директор ООО «Департамент транспортной безопасности», к.т.н.*

В условиях складывающейся обстановки и новых угроз в целях упорядочивания мер по защите объектов транспортной инфраструктуры (ОТИ) от актов незаконного вмешательства (АНВ) с применением беспилотных аппаратов (БПА) в действующее законодательство о транспортной безопасности (ФЗ-16) в 2024 году были внесены необходимые изменения (ФЗ-2 от 30.01.2024). Кроме того, был принят ряд подзаконных нормативных правовых актов (постановление Правительства РФ от 30.04.2025 № 588, приказ Минтранса России от 24.07.2024 № 255 и пр.).

Вместе с тем существует ряд нормативных коллизий, существенно ограничивающих возможности по защите ОТИ от БПЛА.

ВИДЫ ПРОТИВОДЕЙСТВИЯ БПЛА И НОРМАТИВЫ

Защиту ОТИ от БПЛА по видам противодействия можно условно разделить на **пассивную** и **активную**.

Пассивная защита ОТИ включает комплекс инженерных систем, устанавливаемых на объекте с целью предотвращения нанесения ущерба. Основные нормативные документы здесь – ФЗ-384 «Технический регламент о безопасности зданий и сооружений» и СП 542.1325800.2024 «Свод правил. Защитные ограждающие конструкции от беспилотных летательных аппаратов. Правила проектирования». Пассивная защита включает в себя:

- улавливающие сетчатые конструкции;
- ограждения из стальных тросов (канатов);
- опоры;
- растяжки;
- тюфяки/маты;
- противоосколочные стенки;
- укрытия для персонала.

Активная защита ОТИ предусматривает обнаружение и пресечение функционирования БПЛА. Основные нормативные документы включают в себя: ФЗ-16 «О транспортной безопасности», постановление Правительства РФ от 30.04.2025 № 588, приказ Минтранса России от 24.07.2024 № 255. Активная защита предусматривает:

- подавление или преобразование сигналов дистанционного управления беспилотными аппаратами;
- воздействие на пульты управления беспилотными аппаратами;
- повреждение или уничтожение беспилотных аппаратов.

При этом важно отметить, что согласно ФЗ-16, статья 12.3 (п. 8.2), пресечение функционирования БПЛА возможно **только для ОТИ, вокруг которых установлены зоны безопасности**.

ОБЛАСТЬ ПРИМЕНЕНИЯ ПОСТАНОВЛЕНИЯ № 588. НОРМАТИВНЫЕ КОЛЛИЗИИ

Постановлением Правительства РФ № 588 **определены особенности защиты ОТИ от актов незаконного вмешательства с использованием БПЛА.** Эти особенности распространяются на ОТИ, вокруг которых, согласно постановлению Правительства РФ от 03.06.2020 № 814, устанавливаются **зоны безопасности.** Это:

- *для воздушного, железнодорожного, водного и автомобильного транспорта:* ОТИ 1-й и 2-й категорий, или ОТИ, связанные с опасными грузами;
- *для объектов дорожного хозяйства:* **качественные критерии (независимо от категории!)** – это… мосты, эстакады длиной более 100 метров и (или) имеющие пролетное строение длиной более 60 метров и тоннели длиной более 100 метров, для обхода (объезда) которых отсутствуют автомобильные

дороги,…протяженностью до 50 километров с той же или более высокой категорией.

Таким образом: отдельные ОТИ дорожного хозяйства 3-й и 4-й категорий, а в отдельных случаях и некатегорированные (!) **подлежат** установлению зон безопасности и защите от БПА согласно ПП № 588!

При этом **существуют ограничения** для ОТИ 3-й и, особенно, 4-й категорий и некатегорированных ОТИ по их оснащению инженерно-техническими средствами (ИТС) обеспечения транспортной безопасности (согласно ПП РФ № 2201, № 1605 и пр.), привлечению для их защиты сил ОТБ и применению ими оружия в том числе для противодействия БПЛА (ФЗ-16). То есть в соответствии с требованиями законодательства организовать защиту таких объектов от БПЛА невозможно!

ПОСТАНОВЛЕНИЕ № 588. ПРОБЛЕМНЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ

В соответствии с ФЗ-16 «О транспортной безопасности» (статья 2), оценка уязвимости объектов транспортной инфраструктуры является одной из основных задач обеспечения транспортной безопасности.

При этом все дальнейшие действия по защите ОТИ, в том числе по привлечению подразделений транспортной безопасности, осуществляется с учетом проведенной оценки уязвимости и в строгом соответствии **с утвержденным планом обеспечения транспортной безопасности** ОТИ.

Согласно постановлению Правительства РФ № 588, границы и конфигурация зон безопасности ОТИ для защиты от БПЛА устанавливаются субъектами транспортной инфраструктуры (СТИ) на основании утвержденных **результатов оценки (дополнительной оценки) уязвимости**. А защита ОТИ с учетом новых требований, как уже говорилось выше, возможна только после утверждения нового плана ОТБ.

Как показала практика, это трудоемкий и длительный процесс.

В силу сложившейся ситуации отдельные СТИ под давлением надзорных органов, **не дожидаясь проведения оценки уязвимости и утверждения плана ОТБ согласно ПП № 588**, на свой страх и риск вводят в практику защиты ОТИ применение средств обнаружения и пресечения деятельности БПА, **зачастую вменяя эти задачи подразделениям транспортной безопасности**.

При этом пакет организационно-распорядительных документов (ОРД), предусмотренный ПП № 588, **не принимается**, и вся защита организуется на субъективном понимании положений ФЗ-16, ПП № 588 и приказа Минтранса № 255, определившего порядок и способы пресечения функционирования БПЛА.

Такой подход чреват серьезными последствиями в случае ошибочного или некорректного реагирования на реальные БПА!

ПТБ И ПРОТИВОДЕЙСТВИЕ БПЛА: НОРМАТИВНЫЕ ОГРАНИЧЕНИЯ

Актуальным является и необходимость совершенствования нормативной базы, регламентирующей деятельность ПТБ в целях повышения их эффективности по противодействию БПЛА. Так, в числе проблемных вопросов остаются:

- отсутствие правовой защиты работников аккредитованных ПТБ при исполнении обязанностей, в том числе в условиях крайней необходимости (как это, например, предусмотрено для ведомственной охраны);
- ограничение (для аккредитованных ПТБ) в использовании боевого стрелкового оружия для противодействия БПЛА (согласно ФЗ-16, возможно применение только служебного огнестрельного оружия и только для защиты ОТИ 1-й и 2-й категорий);
- отсутствие регламентации порядка защиты от БПЛА (в том числе использования ИТС ОТБ и применения оружия) для ОТИ 3-й и 4-й категорий, а также для некатегорированных ОТИ.

ПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТИ ОТ БПЛА

В части прав и полномочий сил обеспечения транспортной безопасности:

- необходимость внесения изменений в ФЗ-16 «О транспортной безопасности», предусматривающих гарантии правовой защиты работников аккредитованных ПТБ;
- необходимость внесения изменений в законы «Об оружии» и ФЗ-16 «О транспортной безопасности» с целью предоставления возможности для отдельных категорий аккредитованных ПТБ применения боевого стрелкового оружия для защиты ОТИ от БПЛА, **вне зависимости от категорий ОТИ**.

В части установления зон безопасности и реагирования:

- уточнить требования ПП № 814 для объектов дорожного хозяйства, определив необходимость установления зоны безопасности только **для ОТИ 1-й и 2-й категорий**, по аналогии с иными видами транспорта;
- исключить **введение в практику** защиты ОТИ от АНВ организационно-технических мероприятий по пресечению деятельности БПА **до утверждения соответствующих изменений в планы ОТБ**, согласно ПП № 588.

РЕКЛАМА

ПРОТИВОДЕЙСТВИЕ НОВЫМ УГРОЗАМ ДЛЯ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ

Современный аэропорт – это уже не просто транспортный узел, а сложная система, где пересекаются пассажиропотоки, грузовые цепочки, санитарные процессы, топливная инфраструктура, цифровые сервисы и службы безопасности. И чем сложнее система, тем шире спектр угроз, которые она должна отражать. Традиционная логика авиационной безопасности строилась вокруг контроля доступа и обнаружения опасных предметов. Металлодетекторы, рентгеновские интроскопы, досмотр багажа – все это работает, но сегодня этого уже недостаточно.

ПОЧЕМУ ПРИВЫЧНЫЕ СРЕДСТВА НЕ ВИДЯТ НОВЫЕ УГРОЗЫ

Биологические агенты, токсины, аэрозоли и нелицензированные беспилотники – это угрозы, которые не выявляются стандартными процедурами досмотра. Металлодетектор не обнаружит биологический аэрозоль, рентген багажа не покажет патогенные микроорганизмы, сканеры тела не распознают инфекцию, поскольку термометрия реагирует поздно и неспецифично.

Как отмечается в материалах межотраслевой конференции «Противодействие угрозам биологического, химического и радиационного терроризма на объектах инфраструктуры воздушного транспорта» (Москва, июнь 2026 года), объектом наблюдения должен стать не только человек или предмет, но и среда аэропорта.

Биологическая угроза может проявляться в воздухе терминала, на контактных поверхностях, в вентиляционных фильтрах и сточных водах. Причем речь идет не только о живых возбудителях, но и о токсинных рисках, которые могут не сопровождаться живым агентом. Существует и проблема неизвестных генетических сигнатур – агентов, для которых отсутствуют стандартные ПЦР-праймеры и референсные библиотеки.

НЕЛИЦЕНЗИРОВАННЫЕ БПЛА: УГРОЗА, ТРЕБУЮЩАЯ ПРОЦЕДУРНОГО ПОДХОДА

Отдельная категория – беспилотники вблизи взлетно-посадочной полосы, глиссады, перрона или топливной инфраструктуры. Здесь важно понимать: любое средство реагирования само может стать источником риска, если создает помехи связи, навигации или работе органов управления воздушным движением.



Комплекс «Сегмент-Гамма» в аэропорту

Поэтому критичным является не «перехват» как таковой, а управляемый цикл: обнаружение, классификация, идентификация, оценка риска и передача решения уполномоченным службам. Высокая доля ложных целей (птицы, отражения, легитимные воздушные объекты) требует мультисенсорной проверки, а не автоматического перевода сигнала в статус угрозы.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПОМОЩНИК, А НЕ ЗАМЕНА

В этой архитектуре искусственный интеллект выполняет роль доверенного слоя слияния данных, проверки гипотез и приоритезации действий. Он объединяет видеоаналитику, радиочастотные признаки, данные радиолокации, контроль доступа, санитарные сигналы и операционные журналы.

Но важно подчеркнуть: ИИ не должен быть автономным субъектом силового или санитарного решения. Его задача состоит в формировании проверяемой рекомендации с уровнем уверенности и объяснением признаков. При низкой уверенности система должна снижать уровень автоматизма и передавать событие на ручной разбор.

КАК ЭТО СВЯЗАНО С ТЕХНОЛОГИЯМИ ОБНАРУЖЕНИЯ

Эффективная защита аэропорта требует перехода от реактивного досмотра к проактивному мониторингу среды. И здесь на первый план выходят технологии, способные фиксировать слабые сигналы до того, как они приведут к нарушению безопасности полетов.

Один из примеров такого подхода – автоматический обнаружитель биоаэрозолей **«Сегмент-БИО»**. Он обеспечивает непрерывный анализ воздуха в режиме 24/7, фиксирует частицы размером от 1 до 10 микрометров (бактерии, вирусы, токсины) и выдает сигнал в течение 15 секунд. Это не замена лабораторной диагностике, а инструмент раннего предупреждения, который позволяет запустить регламентированный процесс уточнения: повторный отбор, лабораторную проверку, локальную санитарную меру.



Автоматический обнаружитель биоаэрозолей «Сегмент-БИО»

Для контроля химических угроз в воздушной среде применяется газосигнализатор **«Сегмент»**. Он обнаруживает аварийно химически опасные вещества (хлор, аммиак, сероводород) и боевые отравляющие вещества (зарин, зоман, VX, иприт) с быстродействием до 5 секунд.

А комплекс **«Сегмент-Гамма»** объединяет химический, биологический и радиационный каналы контроля в единой системе.

На входных группах и в зонах досмотра задачи обнаружения следов взрывчатых и наркотических веществ решают портативные детекторы **«Кербер-Т»** и рамановские спектрометры **«ХимЭксперт-Т»**. Первый фиксирует следовые количества на поверхностях, руках и одежде, второй позволяет идентифицировать вещества через прозрачную упаковку без контакта с содержимым.

ЧТО ЭТО ДАЕТ ОБЪЕКТУ

Своевременное выявление биологической или химической угрозы переводит реакцию из режима «ликвидация последствий» в режим «предотвращение». Слабый сигнал не должен автоматически порождать публичную тревогу или остановку терминала, он должен запускать процесс уточнения. И именно скорость получения этого сигнала становится критическим фактором.

Современная система безопасности аэропорта должна отвечать не только на вопрос «Что произошло?», но и на вопрос «Как быстро мы узнаем, что произошло нечто, требующее проверки?». Технологии мониторинга среды – это тот слой защиты, который позволяет увидеть невидимое и выиграть время.

ГК «ЮПХ» разрабатывает и производит оборудование для обнаружения химических, биологических и радиационных угроз. Эти приборы применяются на объектах транспортной инфраструктуры, включая аэропорты Шереметьево, Пулково и Сочи. ■

Андрей Обидин, и. о. заместителя генерального директора, заместитель начальника отдела обеспечения безопасности, ответственный за выполнение мероприятий по АТЗ ФГУП ГосНИИ ГА, кандидат биологических наук;
Дмитрий Сазонов, коммерческий директор ГК ЮПХ (ООО «Модус» и ООО «ЮПХ»)

ПОСТАНОВЛЕНИЕ № 588: ПРАВОВОЙ ФУНДАМЕНТ СОЗДАН – НУЖНА ИНЖЕНЕРНАЯ ОПОРА

Постановление Правительства РФ от 30.04.2025 № 588 закрепило правовой статус защиты объектов воздушного транспорта от БВС, границы зон безопасности и полномочия подразделений транспортной безопасности. Однако переход от юридической нормы к реальной защищенности аэропорта требует единой инженерной экспертизы. В статье обосновывается необходимость создания отраслевого Центра компетенций по противодействию БВС на базе НЦ-17 ФГУП ГосНИИ ГА.



Анжелика Поликарпова,
директор по развитию авиационных технологий ООО «НЕОСКАН»

Постановление № 588 стало своевременным ответом государства на эскалацию угроз с воздуха. Документ четко определил правовой статус защиты от БВС, закрепил границы зон безопасности – до 5 км по земле и 300 м по высоте – и наделил подразделения транспортной безопасности полномочиями по пресечению угроз. Это принципиальный шаг: обязанность защищаться перестала быть декларацией.

Но следующий вопрос – инженерный. Как именно защищаться? Каким оборудованием? По каким критериям проверять, что оно действительно работает? И как не заблокировать вместе с дроном управление воздушным движением, авиационную радиосвязь и резервные каналы передачи данных?

Именно здесь сегодня возникает главный разрыв – между буквой закона и физикой радиоэлектронной борьбы.

РАЗРЫВ МЕЖДУ ЗАКОНОМ И ФИЗИКОЙ

Постановление № 588 обязывает аэропорты провести инструментальное обследование радиоэлектронной обстановки, сформировать модель защиты и закупить спецсредства. Но в отсутствие единых отраслевых стандартов каждый аэропорт вынужден самостоятельно искать методики, подрядчиков и критерии сравнения. Возникают три системных риска.

Первый – методологическая неопределенность. Обследования, выполненные разными подрядчиками по разным методикам, дают несопоставимые результаты. Инвестиционные решения принимаются на основе неполных данных, а модель угроз нередко превращается в формальный документ.

Второй – закупка «мертвого железа». На рынке сотни решений. Часть формально соответствует техническому заданию, но не справляется с реальными сценариями: роевыми группами, автономными БВС, низкими высотами, помехоустойчивыми каналами управления. Постановление упростило отдельные процедуры, но не создало оперативного механизма верификации эффективности. В итоге акт приемки подписан, а защищенности нет.

Третий – проблема интеграции. Для гражданской авиации критична не только мощность подавления, но и избирательность, и сопряжение с контуром безопасности аэропорта. Закупка «закрытых коробок» ведет к созданию несовместимых систем. Особенно остро это проявляется при массовом внедрении зарубежного оборудования: доля китайских экспонентов на отраслевых выставках уже превышает 40%. Далеко не все такие модули проходят регистрацию в ГКРЧ, имеют открытые интерфейсы и адаптируются под российские стандарты. А неселективное подавление возвращает нас к исходной дилемме: защита от дрона ценой парализации радиоэлектронной инфраструктуры аэропорта.

Для аэропорта такая «защита» означает остановку операционной деятельности: невозможность приема и выпуска воздушных судов, сбои в координации служб, потерю ситуационной осведомленности.

Экономические потери – десятки миллионов рублей в сутки, репутационные риски – долгосрочный отток перевозчиков.

ЦЕНТР КОМПЕТЕНЦИЙ: НЕ НАДСТРОЙКА, А ИНЖЕНЕРНЫЙ ФИЛЬТР

Логика Постановления № 588 неизбежно подводит к созданию независимого экспертного органа – моста между требованиями регулятора и физической реальностью аэропорта. Такой Центр компетенций не должен быть еще одной согласующей инстанцией. Его смысл – дать отрасли единый технический язык и единые критерии качества.

Ключевое условие – независимость от поставщиков. При этом было бы неплохо, если бы Центр был полномочен привлекать технических специалистов разработчиков и интеграторов: не для лоббирования, а для глубокой инженерной оценки.

ПЯТЬ ФУНКЦИЙ, БЕЗ КОТОРЫХ ПОСТАНОВЛЕНИЕ № 588 ОСТАНЕТСЯ НА БУМАГЕ

1 **Экспертиза на входе:** независимая оценка технических заданий на поставку систем противодействия БВС, что позволяет еще на этапе планирования отсечь решения с неприемлемым профилем побочного ущерба, несовместимой архитектурой или недоказанной эффективностью.

2 **Верификация эффективности:** оценка уже установленного оборудования с инструментальным контролем и анализом радиоэлектронной обстановки. Это исключает ситуацию «акт подписан, но система не работает».

3 **Методический базис:** участие в разработке отраслевых стандартов, регламентов, модели угроз и модели защиты. Центр берет на себя классификацию угроз и определение критериев эффективности, снимая данную нагрузку со служб безопасности аэропортов.

4 **Официальные заключения:** результаты экспертизы должны оформляться как юридически значимые документы. Для аэропорта это защита перед проверяющими органами и обоснование инвестиций. Для регулятора – прозрачная картина реальной защищенности отрасли.

5 **Техническая поддержка разработчиков и интеграторов:** помощь в адаптации решений под российские стандарты, проведении испытаний, интеграции с существующими системами безопасности и подготовке предложений по корректировке нормативно-правовой базы – включая сертификацию, регистрацию в ГКРЧ и согласование конфигураций с профильными ведомствами.

ЗАКЛЮЧЕНИЕ

Постановление № 588 создало прочный правовой фундамент. Теперь на нем необходимо возвести инженерную конструкцию. Единый Центр компетенций по противодействию БВС – самый логичный и эффективный шаг для того, чтобы требования закона превратились в реальную безопасность.

Только опираясь на централизованную экспертную площадку, российские аэропорты смогут отсеять неэффективные решения, исключить закупку «мертвого железа» и выстроить защиту, которая будет пресекать угрозы с воздуха, сохраняя бесперебойное и безопасное движение самолетов.

Правовой фундамент заложен. Пора строить инженерную опору. ■

Иллюстрации: ООО «НЕОСКАН»



ТСНК ЗАКРЫВАЕТ КОНТЕЙНЕРНУЮ БРЕШЬ В СИСТЕМЕ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

ООО «Диагностика-М» – российский разработчик, производитель и ключевой поставщик технических систем и средств досмотра для обеспечения безопасности граждан и объектов критической инфраструктуры. Особое место в линейке продукции, выпускаемой компанией под маркой ТСНК, занимают стационарные и мобильные инспекционно-досмотровые комплексы (ИДК) портального типа. На сегодняшний день предприятием реализовано 47 высокотехнологичных ИДК, эксплуатируемых на объектах транспортной инфраструктуры в России и за рубежом. Собственная инженерная школа и большой опыт разработки ИДК послужили фундаментом для создания «Портала-К 7027» – нового комплекса, призванного ответить на угрозу, которую ранее недооценили.



ИДК «Портал-К 7027»

Необходимость разработки такого решения стала очевидной после диверсионной операции «Паутина» в июне 2025 года. Тогда FPV-дроны, которые перевозили в обычных грузовиках и морских контейнерах, атаковали военные аэродромы стратегической авиации в разных регионах страны, в том числе в дальних регионах Российской Федерации. Это стало шоком для всей системы безопасности объектов транспортной и критической инфраструктуры. Год спустя подобный сценарий едва не повторился в Брянской области: украинские спецслужбы планировали скрытно перебросить через границу контейнеры с разобранными дронами, замаскировав их под гражданские грузы. То есть, «спящие» БПЛА, легально или полулегально попадающие в страну и накапливающиеся на складах, перестали быть гипотетической угрозой. Они стали реальной проблемой, требующей немедленного решения.

ЗАКОНОДАТЕЛЬНЫЙ ИМПУЛЬС: ОТ РЕГИОНАЛЬНЫХ ПРАВИЛ ДО ФЕДЕРАЛЬНЫХ НОРМ

Первой на новую угрозу отреагировала Московская область. Постановление Губернатора Московской области от 02.07.2025 № 224-ПГ впервые на региональном уровне обязало владельцев контейнерных площадок оснастить свои объекты инспекционно-досмотровыми комплексами для проверки содержимого контейнеров перед въездом на склад хранения. Документ был призван упорядочить стихийные склады, но на практике поставил операторов перед жестким выбором: либо найти средства на установку ИДК, либо уйти с рынка.

Федеральный центр пошел еще дальше. Указ Президента РФ от 24.08.2026 № 604 «О мерах по обеспечению безопасности объектов критической инфраструктуры» ввел дополнительные требования к обеспечению безопасности подобных объектов и порядок реагирования на выявленные угрозы. В частности, в случае непринятия мер по защите таких объектов, включая «неэффективность реализации мероприятий, непосредственно направленных на пресечение угроз нападения с использованием беспилотных воздушных судов», Правительство получает право ввести временное управление имуществом хозяйствующего субъекта. Фактически речь идет о том, что экономия на оборудовании защиты может стоить бизнесу контроля над активами.

КОНТЕЙНЕР ПРОТИВ КОНТЕЙНЕРА: ТЕХНОЛОГИЧЕСКИЙ ОТВЕТ ТСНК

Именно на стыке этих двух нормативных импульсов и родилась в 2026 году разработка ТСНК –

ИДК «Портал-К 7027». Весь комплекс смонтирован внутри стандартного морского 20-футового контейнера и не требует сборки на месте. Благодаря такой конструкции заказчик получает не строительную площадку с фундаментом и многомесячным монтажом, а уже готовое изделие. Установка на месте эксплуатации занимает два-три дня, еще пара дней уходит на настройку.

Технические параметры «Портала-К 7027» точно соответствуют требованиям, установленным законодателем. Проникающая способность в 270 мм по эквиваленту стали позволяет «просветить» насквозь любой стандартный морской контейнер. Система распознавания материалов дифференцирует не менее трех групп веществ – органику, неорганику и их смеси. Этого вполне достаточно, чтобы с высокой вероятностью выявлять запрещенные вложения, будь то оружие, взрывчатые вещества или компоненты БПЛА, не вскрывая тару и не останавливая грузопоток.

Пропускная способность комплекса – не менее 120 транспортных средств в час. Это важный показатель для логистических терминалов, где простой в очереди на досмотр оборачивается прямыми убытками. Важно и то, что «Портал-К 7027» обходится заказчику почти в два раза дешевле мобильного досмотрового комплекса и почти в три раза дешевле стационарного портального ИДК. Для логистических операторов, которые вынуждены соблюдать жесткие сроки приведения инфраструктуры в соответствие с новыми правилами, такое соотношение цены, скорости развертывания и функциональности оказывается решающим. На сегодняшний день в Московской области уже установлены два ИДК «Портал-К 7027», и реализация данного проекта продолжается.

РЫНОК: МЕЖДУ ПРОНИКАЮЩЕЙ СПОСОБНОСТЬЮ И ЦЕНОЙ

ИДК «Портал-К 7027» вышел на рынок далеко не в вакууме. Здесь уже были представлены различные модели инспекционно-досмотровых комплексов от российских и зарубежных производителей, адресованные логистическим терминалам. Безусловно, ряд предлагаемых решений превосходит «Портал-К 7027» по проникающей способности. Однако 270 мм по стали – это не компромисс, а точный расчет: стандартный морской контейнер не имеет стенок большей толщины, поэтому «избыточная» проникающая способность конкурирующего изделия не дает практического преимущества при досмотре именно контейнеров, однако увеличивает цену самого комплекса.

Что касается ИДК ведущих зарубежных производителей – Rapiscan Systems (США), Smiths Detection (Великобритания) и Nuctech (Китай), то в текущих геополитических условиях прямое приобретение и, что важнее, последующее сервисное обслуживание такого оборудования сопряжено с санкционными рисками и целым комплексом системных ограничений. Например, китайский Nuctech с декабря 2020 года включен в Entity List Минторга США как представляющий угрозу национальным интересам, а в декабре 2025 года Еврокомиссия начала расследование в отношении этой компании по подозрению в получении незаконных субсидий.

Не менее рискован и эксплуатационный контур иностранных производителей: отсутствие локального склада запчастей и сервисной сети означает, что поставка комплектующих из-за рубежа занимает 4–8 недель, что для контейнерного терминала сопоставимо с остановкой бизнеса. У российских производителей ИДК тоже есть свои нюансы: либо слишком короткий срок присутствия компании на рынке, из-за чего качество ее изделий на подтверждено эксплуатацией, либо предлагаемое решение нуждается в дополнительной адаптации под формат контейнерной площадки. Всех этих рисков лишен «Портал-К 7027», разработанный специально для контейнерных терминалов компанией с более чем 30-летней историей и не зависящий от внешних поставок, санкционных решений и зарубежных сервисных центров.

ОТ ИННОВАЦИЙ К ОТРАСЛЕВОМУ СТАНДАРТУ

Как отмечают эксперты рынка, в условиях, когда появление Указа № 604 перевело антитеррористическую защищенность критической инфраструктуры страны из плоскости рекомендаций в плоскость управленческой ответственности, выигрывает не тот производитель, который предложит максимальную проникающую способность или дополнительный анализ содержимого, а тот, кто даст заказчику работающий инструмент в короткий срок, по доступной цене и без строительной «головной боли». Так что с учетом совокупной стоимости владения, логистики, сервиса и соответствия требованиям технологического суверенитета ИДК «Портал-К 7027» имеет все шансы задать отраслевой стандарт не только для контейнерных площадок Московской области, но и для других регионов, которые неизбежно столкнутся с такими же требованиями. Широкое внедрение этой разработки может стать универсальным инструментом для быстрого закрытия опасной бреши, через которую очередная «Паутина» уже не пройдет.

РЕКЛАМА

РАДИОЛОГИЧЕСКИЙ ТЕРРОРИЗМ: ТОНКАЯ ГРАНЬ МЕЖДУ ПАЦИЕНТОМ И ТЕРРОРИСТОМ



Владислав Волков,
заместитель генерального директора по развитию АО «НПЦ «АСПЕКТ»

С момента начала специальной военной операции кратно возросли угрозы совершения актов незаконного вмешательства (далее – АНВ) террористической направленности с применением ядерных и радиоактивных материалов, что подтверждается соответствующими материалами Ространснадзора и МВД России.

Данная угроза была сформулирована и утверждена в рамках совместного приказа Минтранса России, ФСБ России, МВД России от 05.03.2010 № 52/112/134 «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств», с последующим отражением в приказах Минтранса России от 23.07.2015 № 227, от 04.02.2025 № 34.

Однако следует признать, что приобретение и установка сертифицированных систем радиационного контроля на объектах транспортной инфраструктуры (далее – ОТИ) не гарантирует стопроцентной защищенности от указанного вида АНВ террористической направленности.

Данный факт связан с рядом организационно-технических «пробелов», присущих большинству ОТИ, подлежащих обязательному оснащению системами радиационного контроля в рамках исполнения требований по транспортной безопасности (далее – ТБ):

- отсутствие в паспортах обеспечения ТБ моделей угроз в части несанкционированного проноса и провоза на ОТИ ядерных и радиоактивных материалов;
- отсутствие методик реагирования на факт обнаружения при проведении процедур досмотра, дополнительного и повторного досмотра ядерных и радиоактивных веществ и материалов;
- отсутствие в структурах подразделений транспортной безопасности (далее – ПТБ) подготовленных специалистов в области радиационной, химической, биологической защиты.

В части угроз радиологического терроризма принято выделять три основных категории:

1 Использование радиоактивных веществ в составе устройств диспергирования, включая «грязную бомбу».

2 Размещение радионуклидных источников большой активности в местах постоянного и массового пребывания людей.

3 Помещение радионуклидных источников большой активности в технологическое оборудование и процессы, что приводит к радиоактивному загрязнению окружающей среды, промышленных и социально значимых объектов (склады с продуктами питания, станции водоподготовки и т. д.).

В части ОТИ и ТС наиболее актуальными являются угрозы радиологического терроризма первой и второй категорий.

Анализ эксплуатируемых на ОТИ систем радиационного контроля показывает, что большинство «тревожных событий», сформированных радиационными мониторами, связано с проходом через границу зоны транспортной безопасности физического лица, проходившего лечение от онкологического заболевания с помощью радиофармпрепаратов. Эти препараты активно применяются в специализированных клиниках как на территории РФ, так и за рубежом.

С точки зрения норм ТБ, физическое лицо не является террористом в случае наличия у него законного основания в лице официальной справки, выданной специализированным медицинским учреждением, которая подтверждает факт лечения конкретным типом радиоактивного материала. При этом в справке в обязательном порядке должно быть указано наименование радиоактивного материала.

На большинстве ОТИ реагирование на факт срабатывания радиационного монитора ограничивается проверкой представителем сил ПТБ справки и внесением соответствующей записи в журнал. При этом подтверждение наличия у физического лица указанного в справке радиофармпрепарата не осуществляется ввиду отсутствия на ОТИ радиометров-спектрометров, позволяющих проводить процедуры дополнительного и повторного досмотра в целях локализации и распознания его типа и наименования.

Проход на ОТИ онкобольного физического лица – наиболее вероятный сценарий срабатывания систем радиационного контроля на ОТИ без признаков подготовки и совершения АНВ, но при этом в моделях угроз должна быть отражена модель проноса на ОТИ источников большой активности под видом онкобольного, имеющего необходимую, самостоятельно напечатанную справку. В данном случае сценарий сверки справки без полного дополнительного досмотра приведет к совершению АНВ на ОТИ или к беспрепятственной перевозке источника в другой регион для совершения АНВ.

Следует понимать, что на территории, подконтрольной Украине, сосредоточено значительное количество радиоактивных отходов, которые могут быть применены в качестве поражающих элементов при совершении АНВ.

Отдельно следует подчеркнуть, что этот поражающий элемент будет выглядеть не как бочка объемом 200 литров, а как небольшой предмет с габаритными размерами меньше коробка от спичек, не обладающим какими-либо признаками угроз, которые могут быть обнаружены системами досмотра, кроме радиационных мониторов.

Отдельно необходимо рассмотреть вторую категорию угрозы радиологического терроризма – «размещение радионуклидных источников большой активности в местах постоянного и массового пребывания людей».

Ранее, в соответствии с пунктом 8 постановления Правительства РФ от 23.01.2016 № 29, «на период строительства застройщик был обязан организовать на строящемся объекте транспортной инфраструктуры досмотр в целях обеспечения транспортной безопасности, пропускной и внутриобъектовый режимы, обеспечивающие контроль за входом (выходом) физических лиц, въездом (выездом) транспортных средств, вносом (выносом), ввозом (вывозом) грузов и иных материальных объектов, в том числе в целях предотвращения возможности размещения или попытки размещения взрывных устройств (взрывчатых веществ), загрязнения опасными химическими, радиоактивными или биологическими агентами, угрожающими жизни или здоровью персонала и других лиц».

По прошествии четырех лет, в рамках обновленного постановления Правительства РФ от 31.12.2020 № 2418, формулировка значительно видоизменилась: «…пропускной и внутриобъектовый режимы, обеспечивающие контроль за входом (выходом) физических лиц, въездом (выездом) транспортных средств, вносом (выносом), ввозом (вывозом) грузов и иных материальных объектов, в том числе в целях предотвращения возможности размещения или попытки размещения взрывных устройств (взрывчатых веществ), угрожающих жизни или здоровью персонала и других лиц».

Анализ двух документов, цель которых – обеспечение требований в области ТБ на этапе строительства, показывает осознанное занижение требований в части угроз радиологического терроризма. Постановление Правительства РФ от 31.12.2020 № 2418 действует до 1 января 2027 года, и, возможно, указанная коллизия будет устранена при подготовке новой редакции НПА.

Исходя из вышесказанного, можно сделать вывод о необходимости разработок единых моделей угроз и методик реагирования, без которых невозможно построить эффективную систему противодействия актам радиологического терроризма на ОТИ и ТС.

АО «НПЦ «АСПЕКТ» в рамках разработки комплекса АКРК-01М учел опыт ФТС России, пограничного управления ФСБ России в части предотвращения несанкционированного проноса и провоза ядерных и радиоактивных материалов через государственную и таможенную границу РФ.

Комплекс АКРК-01М состоит из стационарных и носимых подсистем радиационного контроля, с помощью которых возможно построить автоматизированную систему с функционалом самодиагностики и поддержки принятия решений, способную обеспечить построение стандартизированного алгоритма действия и реагирования на факт обнаружения на границе зоны транспортной безопасности ядерных и радиоактивных материалов (альфа-, бета-, гамма-, нейтронного излучения).

Специалисты АО «НПЦ «АСПЕКТ» всегда готовы обеспечить оперативную поддержку в части подбора, проектирования, внедрения и дальнейшего сопровождения сертифицированной аппаратуры радиационного контроля вне зависимости от типа объекта.

РЕКЛАМА

РАДИОСВЯЗЬ В АЭРОПОРТАХ: УСТОЙЧИВОСТЬ, БЕЗОПАСНОСТЬ И НЕЗАВИСИМОСТЬ ИНФРАСТРУКТУРЫ

Аэропорт – один из наиболее сложных и высоконагруженных объектов транспортной инфраструктуры, где безопасность и бесперебойность технологических процессов выступают безусловным приоритетом. На территории аэропорта функционирует комплекс специализированных служб – ОрВД, САБ, СПАСОБ, ПДСА, ЭСТОП и другие, – каждая из которых решает критически важные задачи и должна взаимодействовать с остальными в режиме реального времени. Их круглосуточная работа выстроена как высокоточный механизм: сбой или задержка на одном участке способны вызвать каскадные нарушения во всей системе. В этих условиях радиосвязь – не вспомогательный инструмент, а базовый канал оперативного взаимодействия, от которого напрямую зависит устойчивость работы аэропортового комплекса.



Климентий Печенкин,
руководитель проектных продаж
ООО «ЮНИЛОУД»

Организация радиосвязи в современном аэропорту – задача повышенной сложности. Необходимо обеспечить четкое разделение каналов и отсутствие взаимных помех между службами, работающими в разных зонах (терминалы, перрон, летное поле, зоны ограниченного доступа) и с разными приоритетами трафика. К оборудованию предъявляются повышенные требования по надежности, отказоустойчивости, резервированию, защите от электромагнитных помех, устойчивости к климатическим воздействиям, а также по соответствию отраслевым нормативам в области транспортной безопасности и авиационной электросвязи.

На протяжении последних 30 лет аэропорты активно эксплуатировали иностранное оборудование радиосвязи. Такая практика сложилась на фоне утраты собственных компетенций в разработке и производстве средств радиосвязи в России. Сегодня эта зависимость превратилась в системную уязвимость. Ряд производителей полностью прекратил поставки, другие существенно увеличили сроки поставки оборудования. Попытки заместить освободившуюся нишу за счет иных иностранных поставщиков лишь смещают зависимость, не устраняя ее: ключевые транспортные объекты по-прежнему остаются уязвимыми перед внешними факторами.

Особую сложность создает ситуация с радиостанциями в авиационном диапазоне. До введения ограничительных мер такие устройства поставлялись преимущественно из Японии. В текущих условиях их ввоз возможен только по каналам параллельного импорта – полностью или частично. Это ставит под угрозу предсказуемость эксплуатации и сервисного сопровождения: отсутствие гарантированных поставок запчастей, недоступность

обновлений программного обеспечения, прекращение технической поддержки и невозможность проведения регламентного обслуживания создают реальные риски для непрерывности технологических процессов.

С точки зрения регуляторных требований ситуация усугубляется. Современные нормы транспортной безопасности предполагают обязательный аудит радиообмена, фиксацию переговоров, разграничение прав доступа и наличие доказательной базы для расследований инцидентов. Аналоговые системы и ряд устаревших цифровых решений не обеспечивают необходимый уровень прозрачности и контроля, что формирует дополнительные регуляторные риски для эксплуатанта. Для руководства аэропорта и службы безопасности это не «технические нюансы», а прямые риски несоответствия требованиям, штрафов и приостановки деятельности.

В этих условиях особую ценность приобретают решения, устойчивые к внешнему давлению и обеспечивающие долгосрочную техническую поддержку на территории России. Компания «ЮНИЛОУД» взаимодействует с одним из крупных мировых брендов в сфере радиосвязи – Kirisun, а также с его эксклюзивным дистрибьютором в России – компанией «НЕОКОМ». Kirisun официально представлен на российском рынке и располагает полноценной технической поддержкой, складом ЗИП и обученным инженерным персоналом, что делает его одним из наиболее устойчивых инструментов в текущих условиях.

Совместно с «НЕОКОМ» компания «ЮНИЛОУД» предлагает комплексные решения по обновлению систем технологической цифровой радиосвязи в аэропортах. В основе предложений – оборудование Kirisun и программные продукты «НЕОН» от «НЕОКОМ», позволяющие выстроить современную, отказоустойчивую и управляемую систему связи, адаптированную под специфику аэропортовой инфраструктуры. Платформа поддерживает централизованное администрирование, гибкое распределение прав доступа, интеграцию с системами диспетчеризации и видеонаблюдения, а также функции цифровой регистрации переговоров, геопривязки абонентов и автоматизированного оповещения. Российское диспетчерское программное обеспечение «НЕОН» включено в реестр Минцифры России (реестровая запись № 18478 от 09.08.2023).

Инвестиции в модернизацию систем радиосвязи следует рассматривать не как операционные расходы, а как стратегические вложения в устойчивость и безопасность объекта. Их целесообразность подтверждается следующими факторами:

- **Снижение операционных и регуляторных рисков.** Цифровая система с функциями приоритезации вызовов, регистрации переговоров и аудита радиообмена минимизирует вероятность ошибок из-за помех или недопонимания, а также обеспечивает соответствие требованиям транспортной безопасности.
- **Предсказуемость эксплуатации.** Использование локализованных решений с гарантированной техподдержкой, складом запчастей и регламентами обслуживания позволяет прогнозировать эксплуатационные расходы и исключить риски срывов поставок и недоступности обновлений.
- **Унификация и снижение совокупной стоимости владения (TCO).** Переход на единую платформу сокращает затраты на обслуживание разнородного парка оборудования, уменьшает потребность в запасных частях и снижает трудозатраты персонала.
- **Масштабируемость и поэтапное внедрение.** Платформа поддерживает поэтапное развертывание без остановки работы аэропорта, что позволяет распределить капитальные затраты по этапам и начать с наиболее критичных участков (например, перронной зоны или службы ОрВД).

Таким образом, переход на современные локализованные решения – это не просто замена оборудования, а формирование устойчивой инфраструктуры, способной гарантировать безопасность и бесперебойность аэропортовых операций в долгосрочной перспективе. Первым шагом на этом пути может стать экспресс-аудит текущего парка средств радиосвязи с оценкой остаточного ресурса, рисков эксплуатации и стоимости владения. Компания «ЮНИЛОУД» готова предоставить предпроектное обследование, расчет TCO и демонстрацию решений на базе оборудования Kirisun и программно-аппаратного комплекса «НЕОН». Для начала сотрудничества достаточно направить запрос на проведение экспресс-аудита – это позволит сформировать дорожную карту модернизации с учетом специфики вашего объекта и бюджета.

РЕКЛАМА

ГРАНИЦЫ АВТОМАТИЧЕСКОГО ДОСМОТРА

ООО «НПО Спецтехника» присутствует на рынке досмотрового оборудования более двадцати лет. Поставлено свыше полутора тысяч рентгеновских установок марки Di-Scan, которые применяются в более чем 50 аэропортах страны, метрополитенах, на железнодорожных вокзалах, автовокзалах и т. д.



Роман Байчоров,
генеральный директор ООО «НПО Спецтехника»

ИЗМЕНЕНИЕ МЕЖДУНАРОДНЫХ ТРЕБОВАНИЙ

27 марта 2026 года вступили в силу обновленные положения Технических инструкций ИКАО (Doc 9284) о перевозке литиевых батарей. Пассажиру разрешено провозить не более двух портативных зарядных устройств. Заряжать их на борту и питать от них другую технику запрещено. Ограничение по количеству согласовано на международном уровне впервые.

За изменением стоит статистика. Федеральное авиационное управление США подтвердило за 2024 год рекордные 89 инцидентов с задымлением или возгоранием литиевых батарей на борту, а по данным обзора UL Standards & Engagement, собранного от более чем 40 авиакомпаний, в 2025 году именно портативные зарядные устройства вышли на первое место среди источников теплового разгона.

ПРИМЕНЕНИЕ НОРМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Росавиация подтвердила действие обновленных норм ИКАО для российских перевозчиков. С последствиями отрасль уже столкнулась: 22 февраля 2026 года на рейсе Екатеринбург – Стамбул вскоре после взлета загорелся аккумулятор в салоне, после чего ведомство предложило Минтрансу ограничить использование зарядных устройств в полете.

Для службы досмотра существеннее другое. Единого порога у перевозчиков нет: часть компаний допускает устройства до 160 Вт·ч, часть ограничивается 100 Вт·ч, различаются и требования к количеству. Нечитаемая маркировка может стать основанием для изъятия, а обнаружение аккумулятора в зарегистрированном багаже, где его перевозить запрещено, допускает вскрытие багажа в отсутствие пассажира.

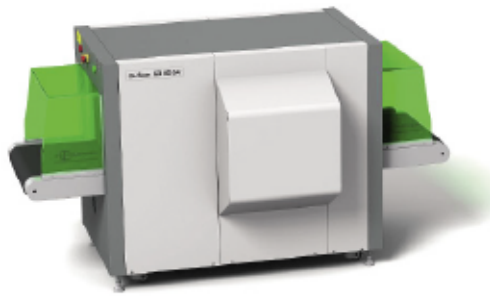
ПОСЛЕДСТВИЯ ДЛЯ ОРГАНИЗАЦИИ ДОСМОТРА

Здесь проходит граница, которую важно обозначить прямо. Автоматическое распознавание решает задачу обнаружения, но не нормоконтроля. Установка формирует изображение по форме, плотности и эффективному атомному номеру: она показывает, что в клади находится литиевый элемент, но не считывает паспортную емкость и не отличает по снимку устройство на 100 Вт·ч от устройства на 160 Вт·ч. Сверка маркировки и оценка соответствия ограничениям перевозчика остаются за инспектором.

Задача автоматики другая: локализовать элемент питания в плотно упакованной кладе, где он теряется среди похожих по геометрии предметов, и вывести его на экран оператора. В багажном потоке, где сплошной ручной контроль невозможен, она становится основной.

МАЛОРАЗМЕРНЫЕ ОБЪЕКТЫ КАК ОБЩАЯ ЗАДАЧА

Схожая динамика характерна и для оружейных угроз. В независимом исследовании From Data to Detection, опубликованном 26 февраля 2026 года в рамках программы Европейского союза EU Global Threats, отмечен относительный рост изъятий деталей и компонентов оружия по сравнению с изделиями в сборе. Такие детали мельче и могут распределяться между



Двухпроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади и багажа Di-Scan 6040 dw



Двухпроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади и багажа Di-Scan 6070 dw

разными местами багажа, а применение полимеров с углеродным наполнением, алюминия и аддитивных технологий дает иную плотность на изображении.

С точки зрения обработки изображения элемент питания и деталь оружия относятся к одному классу задач: малоразмерный объект в загроможденной сцене, который оператор при высоком темпе досмотра пропускает чаще всего.

Второй вывод исследования адресован поставщикам: заявления о возможностях искусственного интеллекта трудно проверить независимо, а качество распознавания определяется объемом обучающих данных, которых по редким объектам не хватает.

АЛГОРИТМЫ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ DI-SCAN

Актуальная версия модели, применяемой в интроскопах Di-Scan, работает со 154 классами предметов, включая литий-ионные аккумуляторы; предыдущие версии распознавали 83 и 146 классов. В основе – сверточные нейронные сети, обрабатывающие двухэнергетическое изображение, а в двухпроекционных установках – оба ракурса. Для жидкостей предусмотрена отдельная модель: она отделяет стенки емкости от содержимого и оценивает его по соотношению сигналов двух энергий и эквивалентному атомному номеру Zef.

Аккумуляторы в этом ряду занимают выгодное положение: в отличие от деталей оружия они есть едва ли не в каждой второй единице ручной клади, поэтому изображений для обучения и проверки накапливается несопоставимо больше, а результат устойчивее.

Каждой единице багажа присваивается статус «Норма» или «Тревога», набор тревожных классов настраивается под требования объекта. Время работы алгоритма не превышает 500 мс на снимок, поэтому он не ограничивает пропускную способность линии. Во внешние системы передаются категория, координаты выделенных областей, уровень уверенности и статус; оборудование может работать в изолированном контуре.

ОГРАНИЧЕНИЯ МЕТОДА

Достоверная идентификация взрывчатых веществ и наркотических средств проекционным рентгеновским методом недостижима: система формирует признак подозрения по форме объекта, характеру упаковки и эффективному атомному номеру, но состав вещества не определяет. Взаимное наложение предметов остается источником ложных срабатываний и пропусков.

Общедоступных отраслевых наборов тестовых изображений не существует, поэтому характеристики обнаружения, приводимые любым производителем, получены на внутренних данных и прямому сравнению не поддаются. Значение имеет проверка на материале конкретного объекта.



Двухпроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади и крупногабаритного багажа Di-Scan 100100 dw

КРИТЕРИИ ОЦЕНКИ ПРИ ЗАКУПКЕ

Отсюда требования, которые целесообразно закладывать в техническое задание и программу испытаний. Проверять систему следует на реальных изображениях заказчика: снимки, накопленные на объекте, обрабатываются моделью без предварительной настройки. Доля пропусков и доля ложных срабатываний приводятся раздельно по каждой категории угроз: усредненная точность мало что говорит о поведении системы на конкретном объекте.

Отдельного обсуждения заслуживает регламент дообучения: кто собирает ошибки, как размечаются данные, с какой периодичностью выходят новые версии модели и входит ли это в договор. В документации фиксируются состав и протокол передачи данных во внешние системы, включая ССОИ.

Нормативная база меняется быстрее, чем обновляется парк оборудования. Заказчику важно понимать, где проходит граница между обнаружением и решением инспектора и как модель будет обновляться в течение всего срока службы установки.

РЕКЛАМА

КОМПЛЕКСНОЕ ОСНАЩЕНИЕ ПУНКТОВ ДОСМОТРА НА ОБЪЕКТАХ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ: КРИТЕРИИ ВЫБОРА И ВЗАИМОДЕЙСТВИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

При оснащении пунктов досмотра на объектах транспортной инфраструктуры наличие необходимого оборудования еще не гарантирует согласованной работы пункта. Арочные и ручные металлодетекторы, интроскопы могут соответствовать техническому заданию по отдельности, но не обеспечивать расчетную производительность при совместной эксплуатации. Основная причина заключается в том, что характеристики приборов оцениваются отдельно от схемы досмотра и условий конкретного объекта.



Илья Анучин, *генеральный директор ООО «Новые Технологии»*

Аэропорты, вокзалы, метрополитены и объекты водного транспорта различаются по интенсивности пассажиропотока, конфигурации входных групп и характеру перевозимого багажа. Даже на объектах одного типа нагрузка на пункты досмотра может существенно отличаться. Поэтому для производителя исходными данными становятся не только категория объекта и перечень необходимых средств, но и план помещения с размерами проходов, распределение пассажиров между входами, пиковые интервалы, порядок проведения досмотра и состав уже установленного оборудования. От полноты этих сведений зависит не только выбор моделей, но и схема их размещения.

Один из наиболее распространенных – определение количества оборудования по среднесуточной посещаемости или паспортной пропускной способности металлодетектора. На практике производительность пункта зависит от последовательности всех операций. Пассажир может быстро пройти через арку, но на подготовку ручной клади к досмотру, анализ изображения или дополнительный досмотр потребуется больше времени. Поэтому расчет ведется по наиболее загруженным периодам с учетом работы сотрудников и возможности вывести пассажира на дополнительный досмотр, не задерживая основной поток.

Не менее важна согласованность досмотра пассажира и его вещей. Арочный металлодетектор предназначен для первичного обнаружения металлических предметов, ручной используется при дополнительном досмотре для их локализации. Интроскоп позволяет досматривать ручную кладь и багаж. Эти средства решают разные задачи, однако их размещение должно обеспечивать понятную последовательность действий: пассажир проходит предусмотренные процедуры, его вещи следуют по соответствующему маршруту, а при необходимости дополнительного досмотра сохраняется возможность продолжать работу основного поста. Избыточное расстояние между участками, неудобное расположение рабочих мест или отсутствие отдельного пространства для дополнительного досмотра снижает эффективность даже правильно подобранного оборудования.

При проектировании необходимо учитывать и особенности входной группы. Металлические ограждения, несущие конструкции, инженерные коммуникации и соседние приборы ограничивают монтажное пространство и могут влиять на условия работы металлодетекторов. Для производителя существенны не только габариты арки, но и расстояния до окружающих конструкций, доступ к органам

управления и возможность технического обслуживания. Именно поэтому решение о размещении оборудования целесообразно принимать до окончательного утверждения технического задания, а не после поставки.

Практический пример индивидуального подбора – оснащение Московского метрополитена оборудованием **RADARPLUS**. Перед компанией «Новые Технологии» стояла задача обеспечить высокую пропускную способность с учетом потребностей маломобильных пассажиров. Для проекта были предложены арочные металлодетекторы **RADARPLUS Model F** с 18 зонами обнаружения, сенсорным экраном и увеличенной до 900 мм шириной прохода. В данном случае определяющим стал выбор исполнения, соответствующего условиям конкретной входной группы. При этом изменение конструктивных параметров должно сохранять установленные характеристики обнаружения и соответствовать области действия сертификата.

Отдельное направление комплексного оснащения – информационное взаимодействие. Современные металлодетекторы передают сведения о срабатываниях и техническом состоянии во внешние системы. В частности, **RADARPLUS Model F** предусматривает обмен данными по Ethernet с использованием формата XML. Однако наличие интерфейса не означает автоматической совместимости с программным обеспечением объекта. До внедрения необходимо согласовать состав передаваемых событий, их привязку к конкретному посту, порядок регистрации и требования к работоспособности при нарушении связи. Передача сигнала тревоги не заменяет установленную процедуру дополнительного досмотра и действий сотрудника.

Нельзя рассматривать комплексное оснащение отдельно от условий дальнейшей эксплуатации. На транспортных объектах оборудование работает при интенсивной нагрузке, поэтому при выборе имеют значение возможность диагностики, доступность комплектующих, сроки ремонта и обучение персонала. Для производителя это также вопрос конструктивной и программной преемственности: техническое обслуживание и возможная модернизация должны выполняться без необоснованного изменения подтвержденных характеристик оборудования. ООО «Новые Технологии» (бренд **RADARPLUS**) использует собственные производственные возможности для подбора исполнения и комплектации, а также обеспечивает техническое сопровождение и обучение сотрудников заказчика.

Обязательным критерием остается соответствие нормативным требованиям. С 1 сентября 2026 года требования к функциональным свойствам технических средств обеспечения транспортной безопасности и правила их обязательной сертификации определяет постановление Правительства РФ № 2107, заменившее № 969. Для ранее сертифицированных единиц оборудования предусмотрено сохранение действия выданных сертификатов на установленный срок службы. При закупке необходимо проверять не только наличие документа, но и его применимость к конкретной модели, исполнению и поставляемому изделию. В линейке **RADARPLUS** представлены арочные и ручные металлодетекторы, имеющие сертификаты соответствия требованиям транспортной безопасности.



Таким образом, комплексное оснащение пункта досмотра начинается с анализа объекта и последовательности предусмотренных процедур. Выбор количества и конфигурации средств, их размещение, передача данных и организация дополнительного досмотра должны рассматриваться как взаимосвязанные решения. Именно такой подход позволяет производителю предложить оборудование, соответствующее нормативным требованиям и реальным условиям эксплуатации, а заказчику – избежать изменений проекта после поставки.

РЕКЛАМА

АППАРАТУРА РАДИАЦИОННОГО КОНТРОЛЯ ДЛЯ ОТИ



РАДИАЦИОННЫЙ МОНИТОР РМ-1СМ-02

Назначение:
Автоматическое обнаружение источников опасных радиоактивных агентов гамма-излучения, перемещаемых физическим лицом через границу зоны транспортной безопасности, в непрерывном режиме.

Технические характеристики:
- Категория радиационного монитора РМ-1СМ-02 по ГОСТ Р 51635-2000 – IVПγ;
- Режим работы: непрерывный, автоматический;
- Климатические условия эксплуатации: температура от -50 до +50 °С;
- Габаритные размеры стойки (Д×В×Ш): (176×764×176) мм;
- Масса: не более 14 кг;
- Энергопотребление: не более 10 В·А.

Внесен в Реестр российской промышленной продукции (ПП РФ 719 от 17.07.2015) под номером 10552032.



РАДИАЦИОННЫЙ МОНИТОР РМ-2СН

Назначение:
Автоматическое обнаружение опасных радиоактивных агентов гамма- и нейтронного излучения, перемещаемых транспортным средством через границу зоны транспортной безопасности, в непрерывном режиме.

Технические характеристики:
- Категория радиационного монитора РМ-2СН по ГОСТ Р 51635-2000 – III Тγ, IV Тn;
- Режим работы: непрерывный, автоматический;
- Климатические условия эксплуатации: температура от -50 до +50 °С;
- Габаритные размеры одной стойки (Д×В×Ш): (350×2018×274) мм;
- Масса стойки: не более 74 кг;
- Энергопотребление: не более 50 В·А.

Внесен в Реестр российской промышленной продукции (ПП РФ 719 от 17.07.2015) под номером 10499964.



РАДИОМЕТР-СПЕКТРОМЕТР УНИВЕРСАЛЬНЫЙ ПОРТАТИВНЫЙ МКС-А03-1

Назначение:
Обнаружение опасных радиоактивных агентов альфа-, бета-, гамма- и нейтронного излучения при проведении процедур дополнительного и повторного досмотра. Локализация опасных радиоактивных агентов. Идентификация опасных радиоактивных агентов гамма-излучения. Хранение и передача обнаруженных и идентифицированных гамма-спектров.

Технические характеристики:
- Степени защиты корпуса прибора: IP65;
- Диапазон рабочих температур: от -20 до +50 °С;
- Габаритные размеры блока МКС-А03 (Д×В×Ш): (280×130×181) мм;
- Масса блока МКС-А03: 3,0 кг.

Внесен в Реестр российской промышленной продукции (ПП РФ 719 от 17.07.2015) под номером 10499962.

ПРОИЗВОДИТЕЛЬ: АО «НПЦ «АСПЕКТ», ТЕЛ./ФАКС: 8 (49621) 6-52-72, 6-51-08; ASPECT@DUBNA.RU, WWW.ASPECT.DUBNA.RU

НПО СПЕЦТЕХНИКА

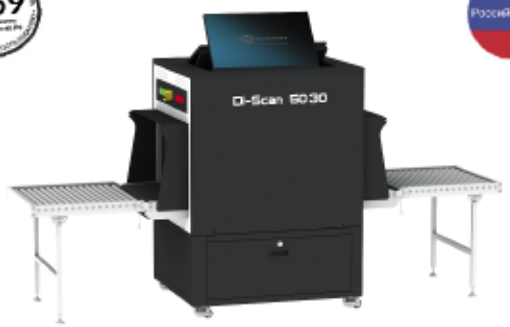
ДОСМОТРОВОЕ РЕНТГЕНОВСКОЕ ОБОРУДОВАНИЕ

Компания ООО «НПО Спецтехника» – ведущий разработчик, производитель и поставщик рентгеновского оборудования торговой марки Di-Scan, позволяющего определять потенциально опасные материалы путем рентгеновского сканирования ручной клади, багажа гражданского населения и крупногабаритных грузов на объектах критической и транспортной инфраструктуры.

Наше предприятие имеет широкую линейку однопроекционного и двухпроекционного досмотрового рентгеновского оборудования (далее – РТУ), состоящую из множества моделей с разными функциональными и техническими параметрами и типовыми размерами как самой РТУ, так и досмотрового туннеля. Также наше предприятие выполняет специальные заказы, удовлетворяя практически любые потребности рынка и обеспечивая соответствие различным требованиям Заказчиков к конструкции установок, применяемому программному функционалу, возможностям интеграции с другими системами безопасности на объектах Заказчиков и установке дополнительных опций.

Ключевыми преимуществами являются высокие технико-эксплуатационные характеристики оборудования наряду с его надежностью, бесперебойным функционированием в любых условиях; использование российского программного обеспечения, в том числе ОС, включенного в единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций РФ. Оперативно осуществляем широкий спектр сопутствующих поставке услуг, начиная от технического, гарантийного и постгарантийного обслуживания, ремонта оборудования и заканчивая модернизацией уже эксплуатируемых установок, обновлением ПО, продлением ресурса, утилизацией. Вся продукция ООО «НПО Спецтехника» обладает быстрым сканированием и интуитивно понятным интерфейсом, что делает ее простой в использовании для операторов и идеальным выбором для организаций, где скорость и эффективность играют важную роль.

Оборудование нашего предприятия соответствует всем действующим нормативным требованиям в Российской Федерации и отвечает международным и отечественным стандартам и требованиям к данному типу оборудования.



Однопроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади и багажа ***DI-Scan 50 30***



Двухпроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади и багажа ***DI-Scan 60 70 dw***



Двухпроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади и крупногабаритного багажа ***DI-Scan 100 100 dw***



Однопроекционная стационарная досмотровая рентгеновская установка конвейерного типа для досмотра ручной клади, крупногабаритного и паллетированного груза ***DI-Scan 150 180***

НПО СПЕЦТЕХНИКА

ПРОИЗВОДИТЕЛЬ (ПОСТАВЩИК):
ООО «НПО Спецтехника»
101000, г. Москва, ул. Мясницкая, д. 47, пом. 4, ком. 1-12
+7 (495) 646-01-01; info@npo-sptech.ru; www.npo-sptech.ru

РЕКЛАМА



МЕТАЛЛОДЕТЕКТОРЫ RADARPLUS -

профессиональные средства досмотра российского производства для объектов с повышенными требованиями к безопасности. Оборудование включено в реестр Минпромторга РФ, отдельные модели соответствуют требованиям транспортной безопасности. Применяются на объектах транспортной инфраструктуры, в аэропортах, на вокзалах, стадионах, промышленных предприятиях и в государственных учреждениях.

+7 495 414-13-55 INFO@RADARPLUS.SHOP RADARPLUS.SHOP

РЕКЛАМА

ТСНК
ООО Диагностика-М

РАЗРАБОТКА И ПРОИЗВОДСТВО ВЫСОКОТЕХНОЛОГИЧНОГО ОБОРУДОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Антитеррористическое оборудование **ТСНК** применяется в аэропортах и метрополитенах, на железнодорожных вокзалах и автобусных станциях, в морских и речных портах, автомобильных пунктах пропуска на Государственной границе Российской Федерации, местах массового пребывания людей и на других объектах, требующих высочайшего уровня защиты. Компания является ведущим российским производителем и поставщиком стационарных и мобильных ИДК для обеспечения безопасности объектов транспортной и критической инфраструктуры.

ИДК «Портал-К 7027» для досмотра морских контейнеров



Изготавливается на базе 20-ти футового контейнера, монтируется на месте эксплуатации за 2 дня. Обладает проникающей способностью 270 мм по эквиваленту стали, распознает в содержимом морских контейнеров нелегальные и опасные грузы, в т.ч. органические, неорганические вещества и их смеси.

Стационарный ИДК «Портал 9232»

Благодаря технологии двухракурсного сканирования обеспечивает сквозной досмотр 100 % движущихся через портал грузовых автомобилей, контейнеровозов и автоцистерн на предмет обнаружения контрабанды, наркотических веществ, боеприпасов и оружия из металлов и углепластиков.



Мобильный ИДК «МИДК 9032»



Обнаруживает контрабанду, нелегальные, опасные предметы и вещества через стальные стены контейнеров и кузовов толщиной до 320 мм. Может быть оперативно развернут для досмотра морских контейнеров, крупногабаритных грузов, и автотранспорта в любой необходимой локации.

Мобильный ИДК «М-СКАН 9032»

Является единственным мобильным комплексом с проникающей способностью до 320 мм по стали, обеспечивающим 100 % защиту персонала. Предназначен для обследования грузов, контейнеров и автотранспорта с целью обнаружения контрабанды, нелегальных предметов и взрывчатых веществ.



РЕКЛАМА

ПРОИЗВОДИТЕЛЬ (ПОСТАВЩИК): ООО «Диагностика-М» 109316, г. Москва, Волгоградский проспект, дом 42
Тел./факс: +7 (495) 228-18-28, E-mail: sale@tsnk.ru, сайт: www.tsnk.ru

Аргут

Там, где нужна связь

Компания «Аргут» – признанный лидер на российском рынке портативных радиостанций (раций). С 2000 года мы самостоятельно разрабатываем, производим и осуществляем продажу современных и высококачественных радиостанций для гражданской радиосвязи.

Мы сумели разработать широкий модельный ряд портативного и возимого оборудования для различных целей и задач: охоты, рыбалки, наземного, воздушного и водного видов транспорта.

В России более 1 000 000 раций «Аргут» используются профессионалами и любителями, а также эксплуатируется различными государственными структурами и коммерческими организациями: аэропортами, производственными предприятиями, в добывающей отрасли и агропромышленном комплексе, торговыми центрами, гостиницами, транспортными компаниями, охранными предприятиями и многими другими.

Российское ПО



Портативная цифровая радиостанция

Аргут А-73



Российское ПО

Возимая цифровая радиостанция

Аргут А-703

СЕРТИФИКАТ БЕЗОПАСНОСТИ • 2107 • РАЗРЕШЕНО К ИСПОЛЬЗОВАНИЮ

Постановление Правительства РФ

Ex



Портативная взрывозащищенная радиостанция

Аргут А-85



запись разговора

Возимая цифровая радиостанция с SFR

Аргут А-1000D

РЕКЛАМА

ООО «АРГУТ»
Адрес: г. Москва,
Дмитровское шоссе, д. 9, стр. 3
INFO@ARGUT.NET
+7 (499) 346-06-32
+7 (800) 555-60-12

НЕОСКАН
ваша безопасность

ТЕХНОЛОГИЧЕСКИЙ ПАРТНЕР
kaspersky

РОССИЙСКИЙ ИНТЕГРАТОР СИСТЕМ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ

ВОЗМОЖНОСТИ СИСТЕМЫ

- Обнаружение и трекинг дрона
- Определение координат пилота
- Классификация дрона
- Идентификация дрона по принципу свой-чужой
- Аналитика и архив инцидентов
- Нейтрализация

Подсистема обнаружения

Подсистема подавления

Подсистема нейтрализации



ООО «НЕОСКАН»

г. Москва, Загородное шоссе, д. 7, к. 5, стр. 1, ком. 303
+7 499 110-22-42
info@neo-scan.ru

РЕКЛАМА

ЮПХ

РУССКИЕ ПРИБОРЫ

НАШЕ ОБОРУДОВАНИЕ **ДЛЯ ВАШЕЙ БЕЗОПАСНОСТИ**



СЕГМЕНТ ГАММА

Непрерывный контроль воздуха в любых помещениях на предмет выявления (обнаружения и идентификации) взрывчатых веществ, опасных химических и биологических агентов.

- Выявление опасных биологических агентов в режиме 24/7
- Выявление и распознавание опасных химических агентов в режиме 24/7
- Выявление и распознавание следовых количеств взрывчатых веществ
- Обнаружение источников гамма-излучения (опционально)

СЕГМЕНТ-БИО

Оперативный контроль и мониторинг биоаэрозолей и микробного загрязнения воздушной среды в любом месте, где требуется защита здоровья и жизни людей.

- Выявление опасных биологических агентов в режиме 24/7



РЕКЛАМА

ПРИГЛАШАЕМ | 15-20 НОЯБРЯ 2025 **ТРАНСПОРТНАЯ НЕДЕЛЯ** | СТЕНД **№ 3.10**

Модус

www.analizator.ru

НАЦИОНАЛЬНЫЕ ЧЕМПИОНЫ
Ассоциация быстрорастущих технологических компаний

Подписывайтесь на наш телеграм канал

@analizator_ru