

Тема 1.3 «Информационное обеспечение в области транспортной безопасности».

Основные понятия и термины

- Информационное обеспечение – комплекс мероприятий и процессов обеспечивающих информационную безопасность
- Информационная безопасность – состояние, обеспечивающее защищённость информационных ресурсов и каналов, а также доступа к источникам информации в целях активного противодействия государства угрозам внедрения в сознание граждан сведений, ориентирующих и мотивирующих их деятельность ведущую, в конечном итоге, к разложению национальной идентичности и размыванию национального суверенитета
- Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- Информационные процессы – сбор, обработка, накопление, хранение, поиск и передача информации
- Информационная система – организационно упорядоченная совокупность документов и информационных технологий, в т. ч. с использованием средств вычислительной техники и связи (автоматизированная система), реализующих информационные процессы.

Основными задачами обеспечения информационной безопасности являются :

- защита информации (в смысле охраны персональных данных, государственной и служебной тайны и других видов информации ограниченного распространения);
- предохранение информации от случайных или преднамеренных воздействий естественного или искусственного характера;
- реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере;
- защищенность потребностей граждан, отдельных групп и населения в целом в качественной информации для их жизнедеятельности, образования и развития, т. е. информационно-психологическая удовлетворенность потребностей граждан и общества в целом и их защищенность от негативных (преднамеренных и случайных) информационно-психологических и информационно-технических воздействий.

Основные мероприятия, обеспечивающие информационную безопасность:

- обеспечение конституционных прав и свобод граждан в области получения информации и пользования ею;
- развитие современных телекоммуникационных систем;
- защита информационных ресурсов от несанкционированного доступа;
- развитие современных информационных технологий, отечественной индустрии информации;
- повышение безопасности информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие отечественного производства аппаратных средств защиты информации;
- защита сведений, составляющих государственную тайну.

Порядок защиты служебной информации определён:

- Постановлением Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
- Закон «О государственной тайне» (в последней редакции от 01.12.2007 № 318-ФЗ)
- Перечнем сведений, отнесённых к государственной тайне, утверждённым Указом Президента российской Федерации от 30 ноября 1995 года № 1203 в последней редакции
- Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности, утверждёнными Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870
- Приказ Минтранса РФ от 16 февраля 2011 г. N 56 «О порядке информирования субъектами транспортной инфраструктуры и перевозчиками об угрозах совершения и о совершении актов незаконного вмешательства на объектах транспортной инфраструктуры и транспортных средствах».

Вся информация с точки зрения права делится на:

- *информацию без ограничения права доступа* - информация общего пользования, информация о состоянии окружающей среды, ее загрязнении, информация в области работ по хранению, перевозке, уничтожению химического оружия и других видах ОМП. Информация, содержащая сведения об обстоятельствах и фактах, представляющих угрозу жизни, здоровью граждан, не подлежит засекречиванию, не может быть отнесена к тайне;
- *информацию с ограниченным доступом* — государственная тайна, коммерческая тайна, банковская тайна, профессиональная тайна и персональные данные как институт охраны права неприкосновенности частной жизни;
- *информацию, распространение которой наносит вред интересам общества, законным интересам и правам граждан.* К ней относится порнография; информация, разжигающая национальную, расовую и другую рознь; пропаганда и призывы к войне; ложная реклама, реклама со скрытыми вставками и т. п.;

- *объекты интеллектуальной собственности* — то, что не может быть отнесено к информации с ограниченным доступом, но охраняется особым порядком через институты интеллектуальной собственности — авторское право, патентное право, средства индивидуализации и т. п. Исключение составляют профессиональные секреты, которые охраняются в режиме коммерческой тайны;
- *иную общедоступную информацию*, среди которой выделяют более 20 видов открытой общедоступной информации.

Информационное обеспечение

работы компетентных органов в области транспортной безопасности включает в себя следующие компоненты:

Результаты оценки уязвимости объектов транспортной инфраструктуры

транспортной безопасности объектов транспортной инфраструктуры

Реестр планов обеспечения транспортной безопасности

Реестр категорированных объектов транспортной инфраструктуры

Реестр специализированных организаций

Порядок обращения со служебной информацией определён:

- Постановлением Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
- Закон «О государственной тайне» (в последней редакции от 01.12.2007 № 318-ФЗ)
- Перечнем сведений, отнесённых к государственной тайне, утверждённым Указом Президента российской Федерации от 30 ноября 1995 года № 1203 в последней редакции
- Перечнем сведений, отнесённых к информации ограниченного распространения, утверждённых приказами руководителей министерств и ведомств России
- Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности, утверждёнными Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870
- Другими нормативными правовыми актами по обеспечению режима секретности в Российской Федерации, а также Перечнем сведений,

Мера ответственности работника за утрату документа или разглашения сведений, содержащихся в документах со служебной информацией ограниченного распространения

- Извлечения из Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

Статья 13.12. Нарушение правил защиты информации

Статья 13.14. Разглашение информации с ограниченным доступом

- Извлечения из Уголовного кодекса Российской Федерации от 27 мая 1996 г. № 63-ФЗ

Статья 275. Государственная измена

Статья 276. Шпионаж

Статья 283. Разглашение государственной тайны

Статья 284. Утрата документов, содержащих государственную тайну

Постановление Правительства Российской Федерации N 1233 от 3 ноября 1994 года

Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"

Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.
2. Установить, что служебная информация, содержащаяся в подготавливаемых в федеральных органах исполнительной власти проектах указов и распоряжений Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, других служебных документов, не подлежит разглашению (распространению).

Председатель Правительства
Российской Федерации
В.ЧЕРНОМЫРДИН

Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти

1. Общие положения

1.1. Настоящее Положение определяет общий порядок обращения с документами и другими материальными носителями информации (далее - документами), содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях (далее - организациях). Положение не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

1.2. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

1.3. Не могут быть отнесены к служебной информации ограниченного распространения:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

1.4. На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка "Для служебного пользования".

1.5. Руководитель федерального органа исполнительной власти в пределах своей компетенции определяет:

- категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;
- порядок передачи служебной информации ограниченного распространения другим органам и организациям;
- порядок снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения;
- организацию защиты служебной информации ограниченного распространения.

1.6. Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных пунктом 1.3 настоящего Положения.

1.7. Служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит разглашению (распространению).

1.8. За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

1.9. В случае ликвидации федерального органа исполнительной власти (организации) решение о дальнейшем использовании служебной информации ограниченного распространения принимает ликвидационная комиссия.

2. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения

2.1. Необходимость проставления пометки "Для служебного пользования" на документах и изданиях, содержащих служебную информацию ограниченного распространения, определяется исполнителем и должностным лицом, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

2.2. Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации.

2.3. Документы с пометкой "Для служебного пользования":

- печатаются в машинописном бюро. На обороте последнего листа каждого экземпляра документа машинистка должна указать количество отпечатанных экземпляров, фамилию исполнителя, свою фамилию и дату печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с отражением факта уничтожения в учетных формах;
- учитываются, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному индексу документа добавляется пометка "ДСП";
- передаются работникам подразделений под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются (тиражируются) только с письменного разрешения соответствующего руководителя. Учет размноженных документов осуществляется поэкземплярно;
- хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

2.4. При необходимости направления документов с пометкой "Для служебного пользования" в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, готовившего документ.

2.5. Исполненные документы с пометкой "Для служебного пользования" группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется пометка "Для служебного пользования".

2.6. Уничтожение дел, документов с пометкой "Для служебного пользования", утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

2.7. Передача документов и дел с пометкой "Для служебного пользования" от одного работника другому осуществляется с разрешения соответствующего руководителя.

2.8. При смене работника, ответственного за учет документов с пометкой "Для служебного пользования", составляется акт приема-сдачи этих документов, который утверждается соответствующим руководителем.

2.9. Проверка наличия документов, дел и изданий с пометкой "Для служебного пользования" проводится не реже одного раза в год комиссиями, назначаемыми приказом руководителя. В состав таких комиссий обязательно включаются работники, ответственные за учет и хранение этих материалов.

В библиотеках и архивах, где сосредоточено большое количество изданий, дел и других материалов с пометкой "Для служебного пользования", проверка наличия может проводиться не реже одного раза в пять лет. Результаты проверки оформляются актом.

2.10. О фактах утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации ставится в известность руководитель организации и назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию.

На утраченные документы, дела и издания с пометкой "Для служебного пользования" составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

2.11. При снятии пометки "Для служебного пользования" на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

Меры ответственности работника за утрату документа или разглашения сведений, содержащихся в документах со служебной информацией ограниченного распространения

- Дисциплинарная ответственность

- Административная ответственность (Извлечения из Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ)

Статья 13.12. Нарушение правил защиты информации

Статья 13.14. Разглашение информации с ограниченным доступом

- Уголовная ответственность (Извлечения из Уголовного кодекса Российской Федерации от 27 мая 1996 г. № 63-ФЗ)

Статья 275. Государственная измена

Статья 276. Шпионаж

Статья 283. Разглашение государственной тайны

Статья 284. Утрата документов, содержащих государственную тайну

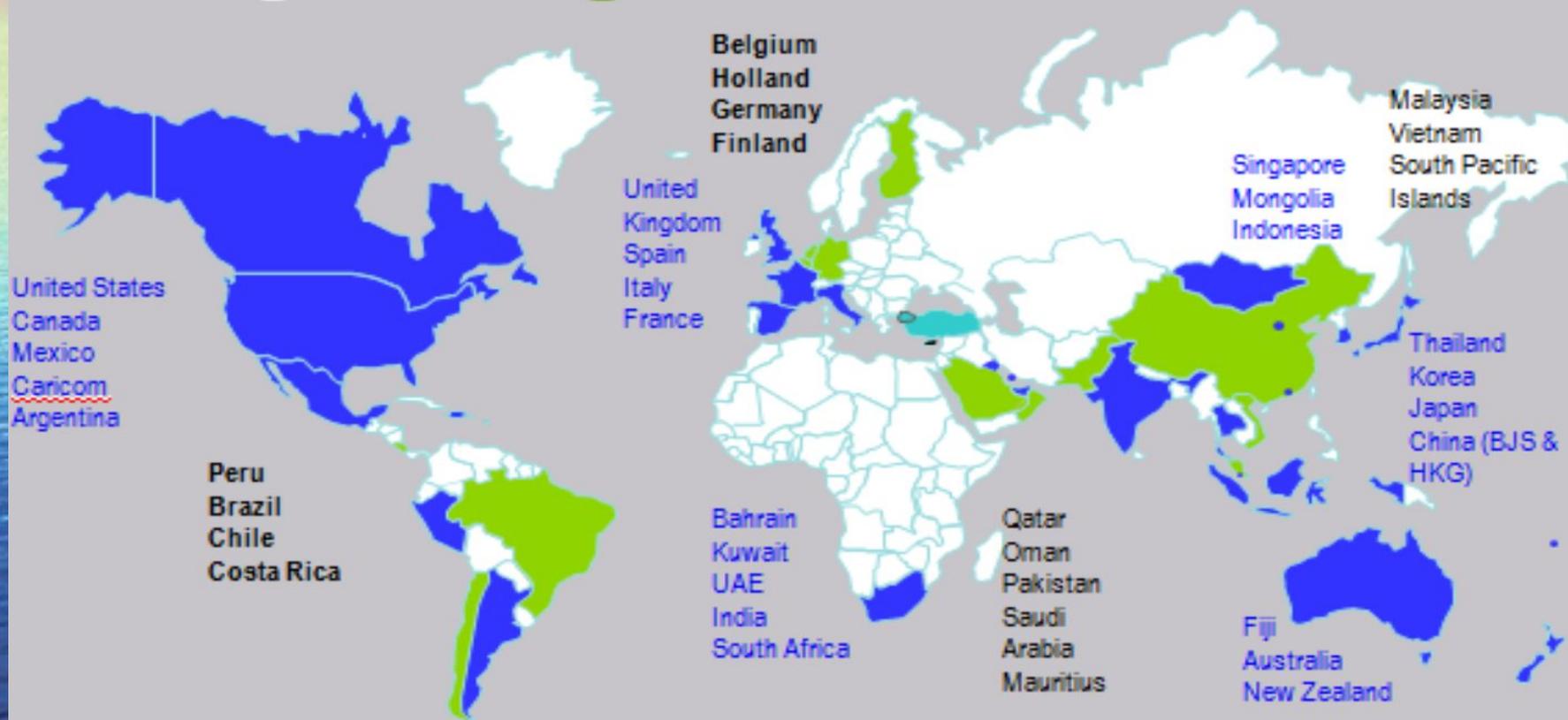
Мировой опыт (продолжение)

Global Passenger Data Requirements

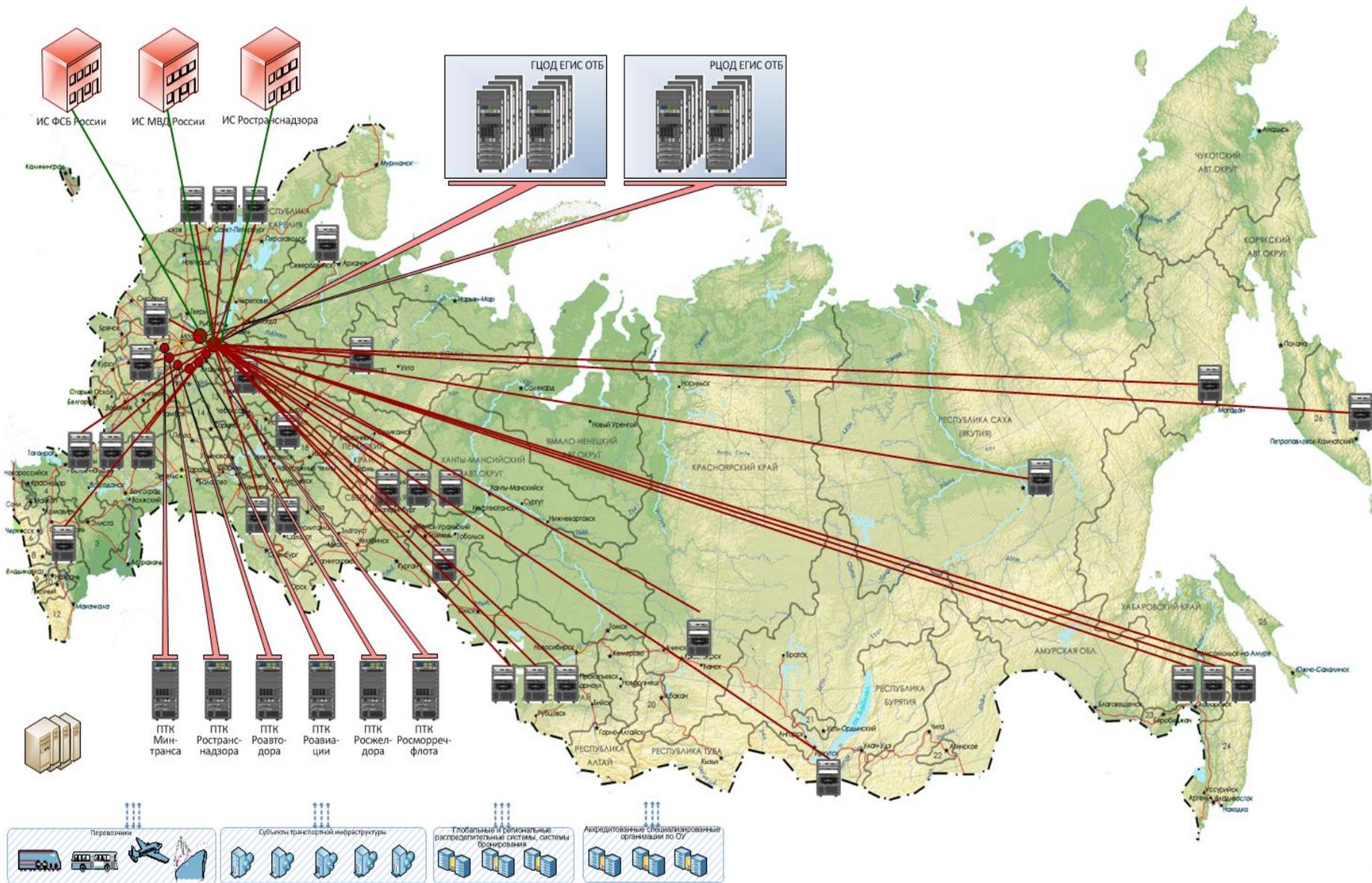
Current



Various Stages



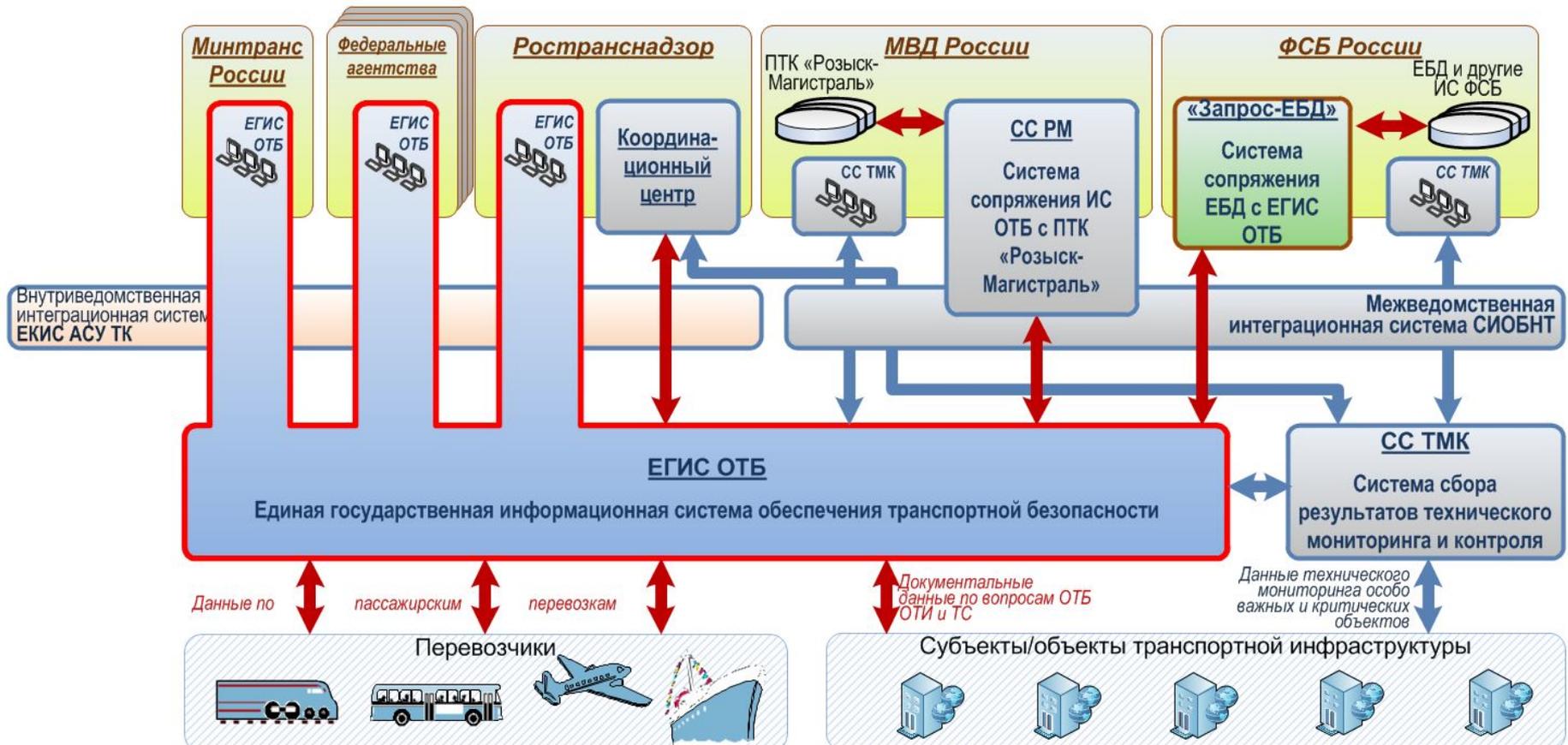
Структурная схема ЕГИС ОТБ



Место ЕГИС ОТБ в системе информационного обеспечения безопасности населения на транспорте (СИОБ)

ЕГИС ОТБ – основа единого защищенного закрытого информационного пространства обеспечения безопасности населения на транспорте.

Создает техническую основу для реализации функций информационного обеспечения деятельности в сфере обеспечения транспортной безопасности в настоящее время, а также в будущем – в указанной сфере и иных сферах транспортного комплекса.



Министерство транспорта Российской Федерации
ФГУП «ЗащитаИнфоТранс»

Объекты автоматизации ЕГИС ОТБ

Объектами автоматизации ЕГИС ОТБ являются федеральные органы исполнительной власти, на которых возложено осуществление полномочий в области транспортной безопасности:

Департамент транспортной безопасности и специальных программ Минтранса России

Управления транспортной безопасности подведомственных Минтрансу федеральных агентств и службы, в т.ч. их территориальные управления

Соответствующие подразделения МВД России и ФСБ России



Структура ЕГИС ОТБ

по функциональному
предназначению – из
компонентов:

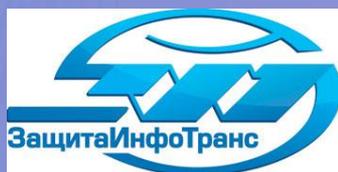
- компонент информационного обеспечения транспортной безопасности (**КИОТБ**);
- компонент персональных данных пассажиров (**КПДП**);
- компонент интеграции данных (**КИД**).

по принадлежности –
из **сегментов:**

- центральный (или сегмент Минтранса России);
- сегмент воздушного транспорта (сегмент Росавиации);
- сегмент железнодорожного транспорта (сегмент Росжелдора);
- сегмент автомобильного транспорта и дорожного хозяйства (сегмент Росавтодора);
- сегмент морского и внутреннего водного транспорта (сегмент Росморречфлота);
- сегмент контроля и надзора на транспорте (сегмент Ространснадзора).

по уровню
конфиденциальности
информации – из
контуров:

- контур персональных данных пассажиров;
- контур конфиденциальной информации;
- контур сведений, составляющих государственную тайну.



Структура информационных компонентов

КПДП
Компонент персональных данных пассажиров

Функциональные подсистемы организации информационного взаимодействия

ШИ Интегрированный вх. шлюз (на базе FTP-сервера)	ШФП Шлюз ФСБ
ШЭ Шлюз ЖД (на базе FTP-клиента)	ШМП Шлюз МВД
ША Шлюз сопряжения с сетями авиа-перевозчиков	ПЗП-А Интерактивное взаимодей. с перевозчиками и субъектами ТИ (Личный кабинет перевозчика)

Транзакционные функциональные подсистемы

ПВИ-В Обработка ПДн пассажиров возд. транспорта	ПМР-В Обработка данных по маршрутам и расписаниям возд. трансп.	ПАС-В Актуализация НСИ воздушного транспорта	ПКП Контроль порядка передачи данных в АЦБПДП
ПВИ-Ж Обработка ПДн пассажиров ЖД транспорта	ПМР-Ж Обработка данных по маршрутам и расписанию ЖД транспорта	ПАС-Ж Актуализация НСИ ЖД транспорта	
ПВИ-А Обработка ПДн пассажиров автотранспорта	ПМР-А Обработка данных по маршрутам и расписаниям автотрансп.	ПАС-А Актуализация НСИ автотранспорта	
ПВИ-М Обработка ПДн пассажиров мор. и речн. трансп.	ПМР-М Обработка данных по маршрутам и расписаниям мор. и вн.водн. трансп.	ПАС-М Актуализация НСИ морского и внутр. водного транспорта	

Комплексная информационно-аналитическая функциональная подсистема

ПЗП-В

Внутренний портал интерактивного взаимодействия с ДЛ Минтранса, агентств, службы (Личный кабинет ДЛ)

- Формирование справок и отчетов
- Комплексный анализ пассажиропотоков
- Доступ к результатам контроля за соблюдением порядка передачи сведений в АЦБПДП

Информационно-технологические функциональные подсистемы

ПБДТ
Формирование и ведение технологических БД

ПБД
Формирование и ведение баз данных по перевозкам

КИД
Компонент интеграции данных

ПВБ-П Ведение архива подлинников	ПРИ-П Ведение реестра субъектов внешних систем источников информации	ПРВ-П Ведение реестра субъектов потребителей информации	ПМД-П Ведение справочника метаданных	ПРО-П Организация распределенной обработки данных	ПОШ-П Реализация общей шины данных	ПРП-П Регистрация и протоколирование сеансов обмена
--	--	---	--	---	--	---

Обеспечивающие подсистемы

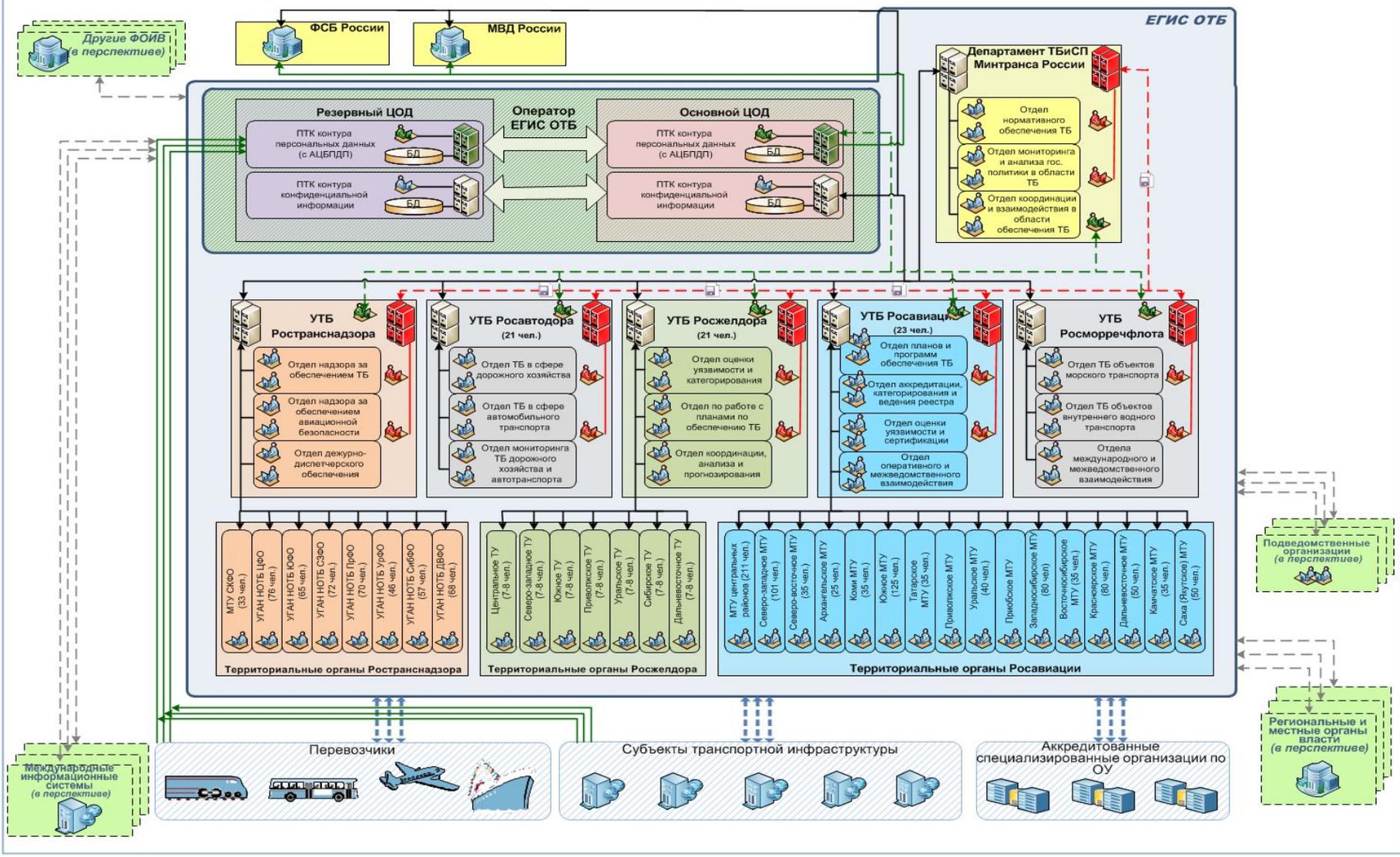
Сервисные подсистемы

ПДН-П Обеспечение доступности и надежности	ПРЗ-П Резервирование и архивирование	ПАУ-П Административное управление	ПСП-П Сопровождение
--	--	---	-------------------------------

Подсистемы обеспечения информационной безопасности

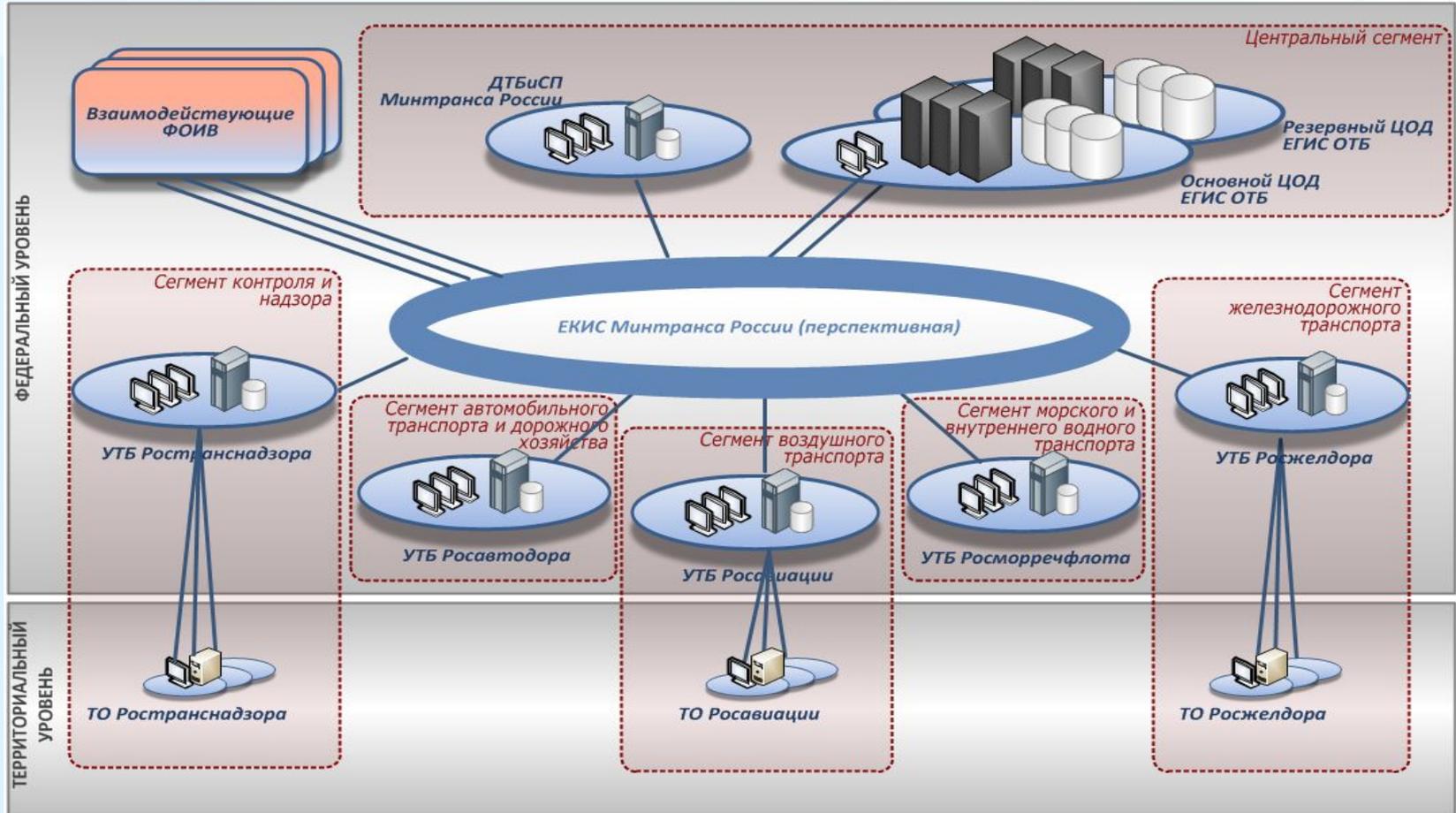
ПИБ-П Прием/передача данных по VPN-каналу	ПИБ-П Сервисы информационной безопасности	УКЦ-П Удостоверяющий и ключевой центр	ПУД-П Разграничение доступа к БДП
---	---	---	---

Организационно-техническая схема ЕГИС ОТБ

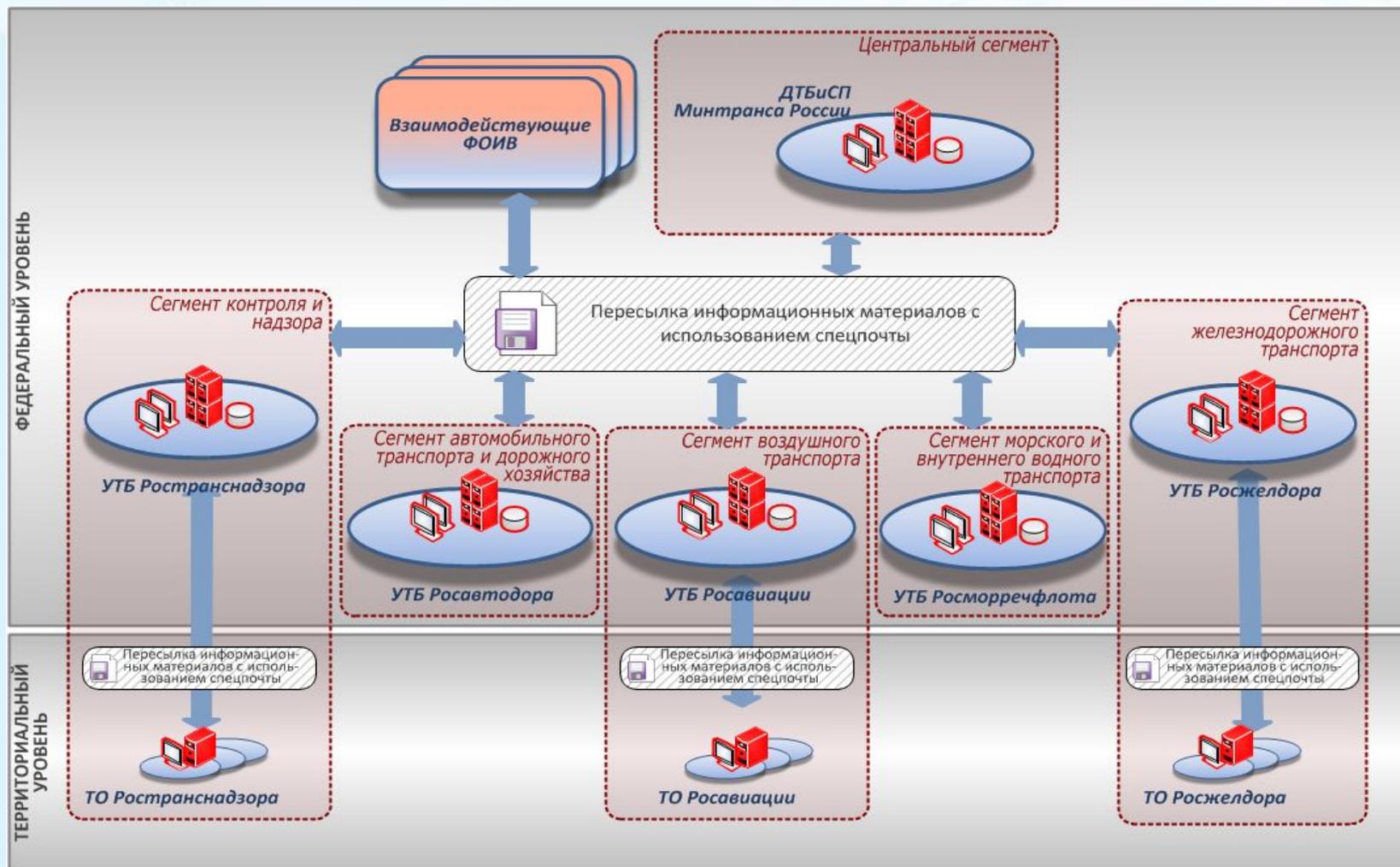


Министерство транспорта Российской Федерации
ФГУП «ЗашитаИнфоТранс»

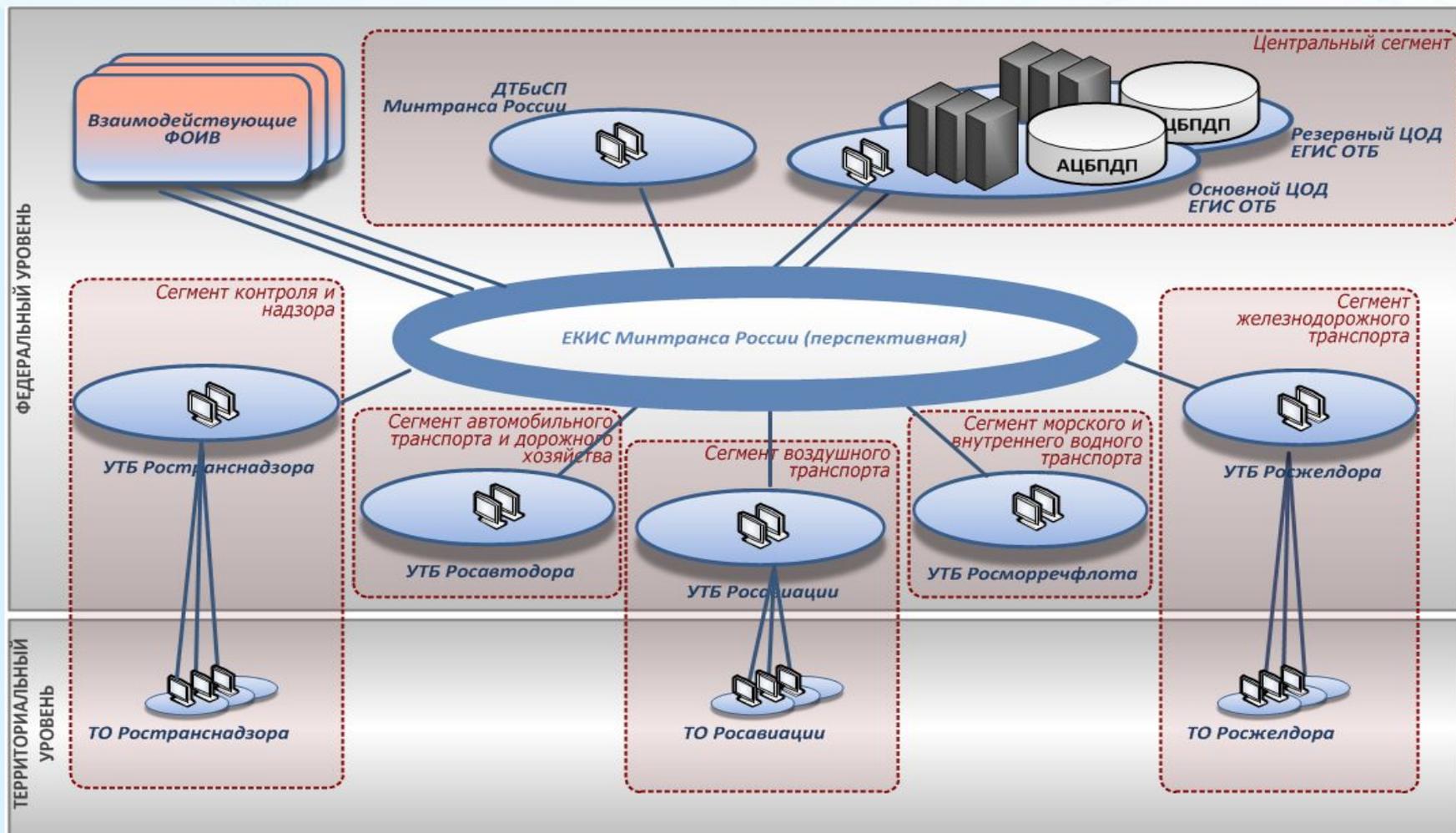
СЕКМЕНТЫ ЕГИС ОТБ (контур К)



СЕГМЕНТЫ ЕГИС ОТБ (контур С – сведений, составляющих гостайну)



СЕКМЕНТЫ ЕГИС ОТБ (контур П – персональных данных)



Единая государственная информационная система обеспечения транспортной безопасности:

1. В целях осуществления мер по обеспечению транспортной безопасности федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере информационных технологий и связи, создана Единая государственная информационная система обеспечения транспортной безопасности, являющаяся собственностью Российской Федерации.

2. Информационная система состоит из автоматизированных централизованных баз персональных данных о пассажирах. Такие базы формируются при осуществлении следующих видов перевозок:

- 1) внутренние и международные воздушные перевозки;
- 2) железнодорожные перевозки в дальнем следовании;
- 3) международные перевозки морским, внутренним водным и автомобильным транспортом;
- 4) перевозки железнодорожным, морским, внутренним водным и автомобильным транспортом по отдельным маршрутам.

3. Автоматизированные централизованные базы персональных данных о пассажирах формируются на основании информации, предоставленной:

- 1) субъектами транспортной инфраструктуры и перевозчиками;
- 2) федеральными органами исполнительной власти;
- 3) иностранными государствами и организациями в рамках международного сотрудничества по вопросам обеспечения транспортной безопасности.

4. Информационные ресурсы Единой государственной информационной системы обеспечения транспортной безопасности являются информацией ограниченного доступа.

5. При оформлении проездных документов (билетов) передаче в автоматизированные централизованные базы персональных данных о пассажирах подлежат следующие данные:

- 1) фамилия, имя, отчество;
- 2) дата и место рождения;
- 3) вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет);
- 4) пункт отправления, пункт назначения, вид маршрута следования;
- 5) дата поездки.

6. Порядок формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах, а также предоставления содержащихся в них данных устанавливается уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

7. Субъект транспортной инфраструктуры или перевозчик иностранного государства, являющиеся собственниками транспортного средства, которое выполняет международные перевозки пассажиров в Российскую Федерацию, из Российской Федерации и (или) через территорию Российской Федерации, либо использующие его на иных законных основаниях, обеспечивают передачу данных, содержащихся в проездных документах (билетах), в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", если международными договорами Российской Федерации не установлено иное.

8. Контроль за соблюдением порядка передачи сведений, предусмотренных настоящей статьей, в автоматизированные централизованные базы персональных данных о пассажирах осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере транспорта.

Виды перевозок, по которым предоставляются ПДн

На основании
части 2 статьи 11
Федерального
закона №16-ФЗ
«О транспортной
безопасности»:

- международных перевозок всеми видами транспорта, в том числе воздушным транспортом:
 - в Российскую Федерацию,
 - из Российской Федерации
 - или транзитом над территорией Российской Федерации (без посадки);
- внутренних воздушных перевозок;
- железнодорожные перевозки в дальнем следовании;
- перевозок по отдельным маршрутам автомобильного, морского и внутреннего водного транспорта (в дальнейшем – по межсубъектовым перевозкам)



Состав персональных данных (ПДн)

Передаваемые в АЦБПДП персональные данные о пассажирах и персонале ТС в соответствии с частью 5 статьи 11 Федерального закона от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» включают:

- Фамилию, имя, отчество;
- Дату рождения;
- Вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет);
- Пол;
- Гражданство;
- Пункт отправления, пункт назначения, вид маршрута следования;
- Дату поездки.
- Дополнительно для экипажа—
должность (роль)

Примечание: В результате поправок в ФЗ «О транспортной безопасности» исключено «Место рождения».



Типы регистрируемых операций при оформлении перевозки железнодорожным транспортом

Бронирование

Приобретение (продажа) билета

Регистрация пассажира

Посадка пассажира на транспортное средство

Возврат билета, отказ от поездки

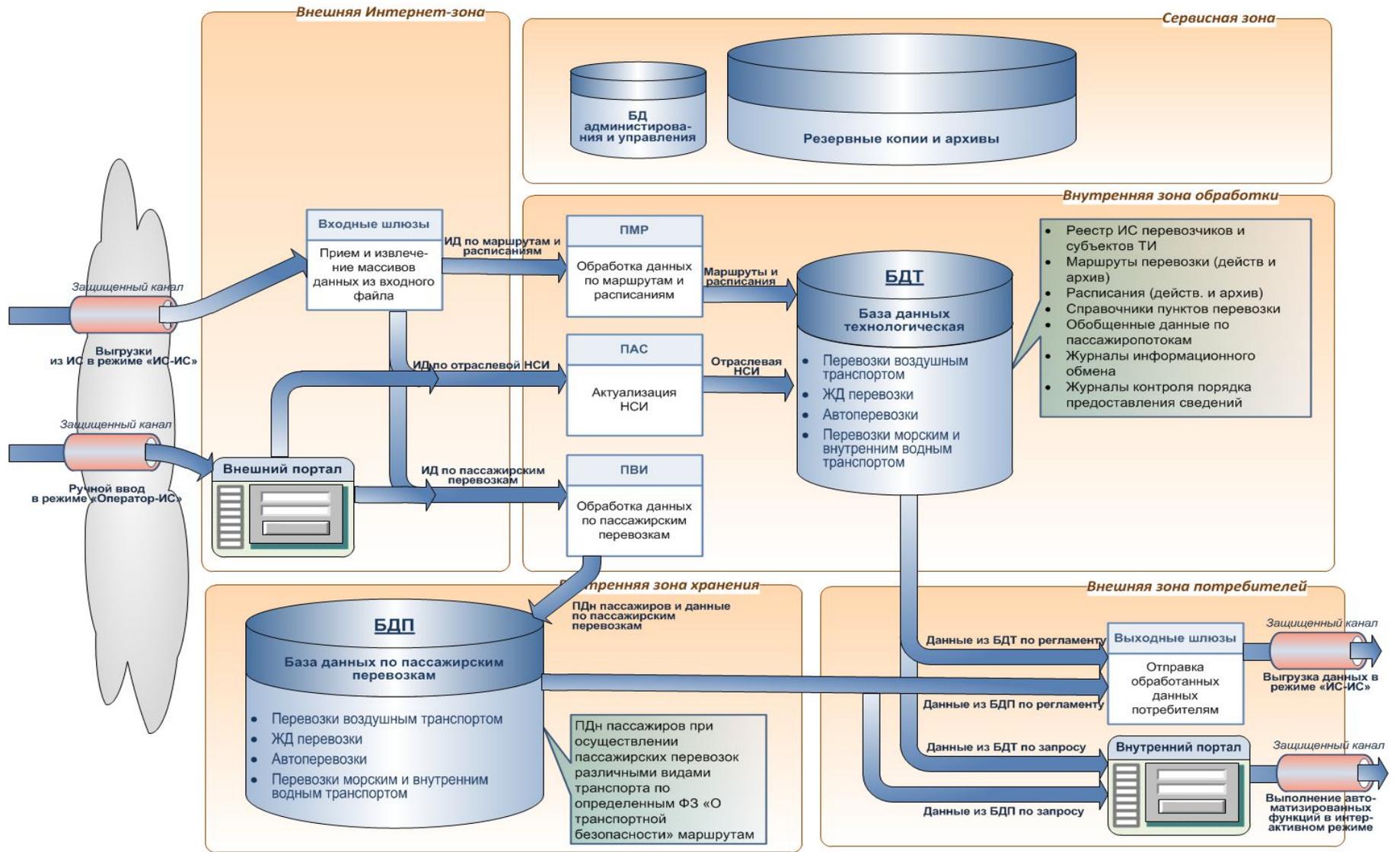
Изменение (переоформление) или прекращение перевозки



В соответствии
с приказом
Минтранса №243
2012 г.
передаваемые в
АЦБПДП данные
содержат сведения
об операции,
регистрируемой в
информационной
системе
перевозчика

- Дата и время операции
- Код операции (бронирование / регистрация / вылет / возврат / ...);
- Наименование или код перевозчика, фактически выполняющего воздушную перевозку;
- Номер рейса;
- Дата и время прибытия воздушного судна;
- Номер бронирования (указатель PNR).

Схема информационных потоков контура «П»



**ПОРЯДОК
ИНФОРМИРОВАНИЯ СУБЪЕКТАМИ ТРАНСПОРТНО
ИНФРАСТРУКТУРЫ И ПЕРЕВОЗЧИКАМИ ОБ УГРОЗАХ
СОВЕРШЕНИЯ И О СОВЕРШЕНИИ АКТОВ НЕЗАКОННОГО
ВМЕШАТЕЛЬСТВА НА ОБЪЕКТАХ ТРАНСПОРТНОЙ
ИНФРАСТРУКТУРЫ И ТРАНСПОРТНЫХ СРЕДСТВАХ**

1. Порядок информирования субъектами транспортной инфраструктуры и перевозчиками об угрозах совершения и о совершении актов незаконного вмешательства на объектах транспортной инфраструктуры и транспортных средствах разработан в соответствии с Федеральным законом от 9 февраля 2007 г. N 16-ФЗ "О транспортной безопасности" и Положением о Министерстве транспорта Российской Федерации, утвержденного Постановлением Правительства Российской Федерации от 30 июля 2004 г. N 395.

2. Субъекты транспортной инфраструктуры и перевозчики обязаны незамедлительно представлять информацию об угрозах совершения и о совершении АНВ на ОТИ и ТС в компетентные органы в области обеспечения транспортной безопасности, Федеральную службу по надзору в сфере транспорта и ее территориальные органы, органы Федеральной службы безопасности Российской Федерации, органы внутренних дел Российской Федерации или их уполномоченные структурные подразделения по средствам электронной или факсимильной либо телефонной связи по адресам (номерам телефонов), указанных на официальных сайтах Федеральной службы по надзору в сфере транспорта и ее территориальных органов.

3. Информирование об угрозах совершения и о совершении актов незаконного вмешательства на объектах транспортной инфраструктуры и транспортных средствах субъектами транспортной инфраструктуры и перевозчиками посредством имеющихся средств связи осуществляется по месту фактического нахождения ОТИ, месту регистрации и фактического нахождения ТС.

4. Субъекты транспортной инфраструктуры и перевозчики при информировании об угрозах совершения и о совершении АНВ на объектах транспортной инфраструктуры и транспортных средствах государственных органов используют телефонные и радиосредства связи, в случае их отсутствия используют электронные и/или факсимильные средства связи.

5. Субъекты транспортной инфраструктуры и перевозчики представляют информацию об угрозах совершения и о совершении АНВ на ОТИ и ТС применительно к конкретным видам транспорта.

6. При отсутствии полной информации об угрозах совершения и о совершении АНВ на ОТИ и ТС, подлежащей представлению, субъекты транспортной инфраструктуры и перевозчики незамедлительно представляют информацию в государственные органы, указанные в пункте 2 настоящего Порядка, и дополняют ее по мере поступления данных.

7. При получении анонимной информации об угрозах совершения и о совершении АНВ на ОТИ и ТС субъекты транспортной инфраструктуры и перевозчики представляют информацию в государственные органы, указанные в пункте 3 настоящего Порядка.

8. При представлении информации об угрозах совершения и о совершении АНВ на ОТИ и ТС в государственные органы, указанные в пункте 2 настоящего Порядка, по средствам телефонной или радиосвязи, в первую очередь называется фамилия, имя и отчество лица, передающего сообщение об угрозах совершения и о АНВ на ОТИ и ТС, занимаемая им должность на ОТИ (ТС), в субъекте транспортной инфраструктуры или перевозчике, их наименование.

Лицо, передавшее сообщение, фиксирует фамилии, имена, отчества, занимаемые должности лиц государственных органов, принявших сообщение об угрозах совершения и о АНВ на ОТИ и ТС, указывает дату и время ее передачи и удостоверяет своей подписью.

9. При представлении информации об угрозах совершения и о совершении АНВ на ОТИ и ТС по средствам электронной связи в электронном виде, информация подписывается электронно-цифровой подписью лица, заполнившего соответствующее приложение к настоящему Порядку (при ее наличии).

10. При представлении информации об угрозах совершения и о совершении АНВ на ОТИ и ТС по средствам факсимильной связи лицо, заполнившее соответствующее приложение к настоящему Порядку на бумажном носителе, удостоверяет его своей подписью.

11. При заполнении соответствующего приложения к настоящему Порядку на бумажном носителе рукописным способом запись производится на русском языке разборчивым почерком или печатными буквами чернилами синего либо черного цвета. Помарки, подчистки и исправления не допускаются.

12. Субъекты транспортной инфраструктуры и перевозчики фиксируют факт передачи, дату и время передачи информации об угрозах совершения и о совершении АНВ на ОТИ и ТС государственным органам, указанным в пункте 2 настоящего Порядка, по средствам электронной, факсимильной связи в соответствии с их программными и техническими средствами.

13. При передаче информации об угрозах совершения и о совершении АНВ на ОТИ и ТС государственным органам, указанным в пункте 2 настоящего Порядка, по средствам телефонной и радиосвязи лицо, передавшее информацию, фиксирует факт ее передачи, дату и время посредством аудио-и/или видеосредств.

14. Срок хранения носителей информации об угрозах совершения и о совершении АНВ на ОТИ и ТС, подтверждающих факт передачи информации, дату и время, а также заполненное соответствующее приложение (приложения) к настоящему Порядку составляет не менее одного месяца.

Представляемая информация об угрозе совершения и о совершении акта незаконного вмешательства в деятельность объекта транспортной инфраструктуры железнодорожного транспорта

1. Дата предоставления информации: Число Месяц Год .
2. Время предоставления информации: Часы Минуты UTC
мск местное.
3. Место получения информации об угрозе
совершения/совершении АНВ (субъект Российской
Федерации, индекс, край, область, город, район, улица, дом).
4. Дата получения информации: Число Месяц Год .
5. Время получения информации: Часы Минуты UTC мск
местное.

6. Реестровый номер категорированного ОТИ: серия, номер.
7. Категория: 1,2,3,4.
8. Наименование собственника или арендатора ОТИ.
9. Адрес местонахождения ОТИ (субъект Российской Федерации, индекс, край, область, город, район, улица, дом)
10. Количество пассажиров, пользователей, посетителей на ОТИ (если есть).
11. Количество персонала на ОТИ.
12. Количество ТС на ОТИ.
13. Тип, модели ТС на ОТИ.
14. Тип, количество груза/багажа, производственных запасов на ОТИ:
15. Количество ТС по типу на ОТИ: локомотив. Пассажирские вагоны, грузовые вагоны, путевая техника (прочее).
16. Другие данные.

Представляемые сведения при получении анонимной информации об угрозе совершения АНВ в деятельность ОТИ железнодорожного транспорта

.Дата предоставления информации: Число Месяц Год .

.Время предоставления информации: Часы Минуты UTC
мск местное.

3. Кто принял информацию: Фамилия Имя Отчество

4. Номер телефона (электронный адрес), принадлежность, место нахождения

средства связи, в адрес которого поступила информация:

Номер телефона, электронный адрес, принадлежность, местонахождение средств связи).

5. Откуда получена информация: Номер телефона, электронный адрес, прочее.

6. Содержание угрозы АНВ.

7. Наличие фонограммы (текста).

8. При получении речевой информации:

8.1. Голос передавшего информацию: мужчина, женщина, подросток, примерный возраст.

8.2. Характер (особенности) голоса: громкий, тихий, высокий, низкий, прочее.

8.3. Речь: быстрая, медленная, отчетливая, искаженная, с заиканием, невнятная, прочее.

8.4. Акцент (выговор): отсутствует, иностранный, диалектный.

8.5. Манера изложения: спокойная, раздраженная, рассудительная, безрассудная, шутливая, непоследовательная, продуманная, эмоциональная, серьезная, прочее.

8.6. Языковой стиль: изысканный, хороший, посредственный, прочее.

8.7. Характер шумов на заднем фоне: уличное движение, оргтехника в офисе, заводской шум, транспорт, музыка, животные, голоса, смешанные шумы, строительный шум, прочее.

Тема 1.3 «Информационное обеспечение в области транспортной безопасности».