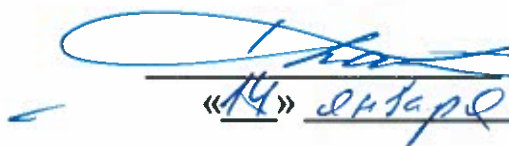


УТВЕРЖДАЮ
Заместитель Министра транспорта
Российской Федерации


Б.М. Ташимов
«14» сентября 2026 г.

Требования
к проведению мероприятий, направленных на создание и апробацию
электронного взаимодействия участников процесса перевозок пассажиров
автомобильным транспортом по межрегиональным маршрутам регулярных
перевозок и исключение бумажного документооборота при организации
таких перевозок, а также требования к обеспечению защиты информации
при проведении эксперимента и информационной безопасности
при использовании информационно-коммуникационных технологий в рамках
эксперимента

1. Общие положения

1.1. Проведение мероприятий, направленных на создание и апробацию электронного взаимодействия участников процесса перевозок пассажиров автомобильным транспортом по межрегиональным маршрутам регулярных перевозок и исключение бумажного документооборота при организации таких перевозок, осуществляется в рамках эксперимента, предусмотренного постановлением Правительства Российской Федерации от 11.11.2025 № 1776 «О проведении эксперимента по обеспечению электронного взаимодействия участников процесса перевозок пассажиров автомобильным транспортом по межрегиональным маршрутам регулярных перевозок» (далее – эксперимент), с использованием Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС».

1.2. Используемые в настоящих требованиях термины и сокращения:

СКПП – программа для электронных вычислительных машин: «Подсистема «СКПП контроля пассажирских перевозок» Государственной автоматизированной информационной системе «ЭРА-ГЛОНАСС»;

ГАИС «ЭРА-ГЛОНАСС» – Государственная автоматизированная информационная система «ЭРА-ГЛОНАСС»;

ФОИВ – федеральный орган исполнительной власти;

ФБУ «Росавтотранс» – федеральное бюджетное учреждение «Агентство автомобильного транспорта»;

АО «ГЛОНАСС» – акционерное общество «ГЛОНАСС», оператор ГАИС «ЭРА-ГЛОНАСС»;

пассажир – физическое лицо, заключившее договор перевозки пассажира, или физическое лицо, в целях перевозки которого заключен договор фрахтования транспортного средства;

перевозчик – юридическое лицо, индивидуальный предприниматель, принявшие на себя по договору перевозки пассажира обязанность перевезти пассажира и доставить багаж в пункт назначения и выдать багаж уполномоченному на его получение лицу;

межрегиональный маршрут регулярных перевозок – маршрут регулярных перевозок в границах не менее двух субъектов Российской Федерации либо в границах одного и более субъектов Российской Федерации и федеральной территории «Сириус»;

рейс – путь транспортного средства по маршруту регулярных перевозок из начального остановочного пункта (первый по времени отправления транспортного средства остановочный пункт, который указан в расписании) в конечный остановочный пункт (последний остановочный пункт, который указан в расписании) или из конечного остановочного пункта в начальный остановочный пункт;

свидетельство на маршрут – свидетельство об осуществлении перевозок по маршруту регулярных перевозок (документ, подтверждающий право на осуществление регулярных перевозок по нерегулируемым тарифам по маршруту регулярных перевозок);

карта маршрута – документ, содержащий сведения о маршруте регулярных перевозок и транспортном средстве, которое допускается использовать для перевозок по данному маршруту;

транспортное средство, автобус, ТС – колесное транспортное средство категории М2 или М3 (за исключением троллейбусов), осуществляющее перевозку пассажиров и багажа по межрегиональному маршруту регулярных перевозок;

ГРН – государственный регистрационный номер транспортного средства;

билет – перевозочный документ, удостоверяющий заключение договора перевозки пассажира;

ОТИ – объекты транспортной инфраструктуры, сооружения, производственно-технологические комплексы, предназначенные для обслуживания пассажиров, фрахтователей, перевозчиков и фрахтовщиков, а также для обеспечения работы транспортных средств;

владелец объекта транспортной инфраструктуры – юридическое лицо или индивидуальный предприниматель, владеющие объектом транспортной инфраструктуры на законном основании;

остановочный пункт, ОП – место остановки транспортных средств по маршруту регулярных перевозок, оборудованное для посадки, высадки пассажиров и ожидания транспортных средств;

расписание – график, устанавливающий время или интервалы прибытия транспортных средств в остановочный пункт либо отправления транспортных средств от остановочного пункта;

уникальный идентификатор – термин используется при совместном упоминании УИП, УИМ, УИР и УИПП, представляет собой цифробуквенную комбинацию, выданную СКПП, однозначно идентифицирующую и объединяющую данные относительно каждого перевозчика, маршрута, рейса и перевозки каждого пассажира или иного лица соответственно при выполнении перевозки автобусом;

УИП – уникальный идентификатор перевозчика;

УИМ – уникальный идентификатор межрегионального маршрута;

УИР – уникальный идентификатор рейса;

УИПП – уникальный идентификатор пассажирской перевозки;

графический интерфейс – разновидность пользовательского интерфейса, в котором элементы интерфейса (меню, кнопки, значки, списки и др.), представленные пользователю на дисплее, исполнены в виде графических изображений;

ПО – программное обеспечение;

Программный интерфейс – описание способов, с использованием которых одна информационная система может взаимодействовать с другой;

смежная информационная система – совместное упоминание информационных систем и источников, являющихся поставщиками данных в СКПП или потребителями данных из СКПП;

СУБД – система управления базами данных;

технология «Госключ» – технология, которая предназначена для создания и использования сертификатов ключей проверки усиленных электронных подписей в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, а также для хранения и применения сертификатов ключей проверки электронных подписей, создаваемых удостоверяющими центрами Казначейства России и ФНС России с использованием мобильных приложений «Госключ» или «Госуслуги»;

АРМ – автоматизированное рабочее место;

СрЗИ – средства защиты информации.

2. Требования к СКПП

2.1. Общие требования

2.1.1. Требования к функционированию СКПП

СКПП должна функционировать в соответствии с установленным коэффициентом готовности СКПП.

2.1.2. Требования к развитию СКПП

СКПП имеет и сохраняет модульную структуру, масштабируемость и возможность дальнейшего развития.

2.1.3. Требования к режимам функционирования СКПП

ПО СКПП должно обеспечивать функционирование СКПП в следующих режимах:

1) штатный – основной режим функционирования. В данном режиме СКПП должна выполнять функции в соответствии с эксплуатационными требованиями;

2) сервисный режим – режим, при котором должны производиться пуск, остановка и перезапуск СКПП, обновление системного и прикладного ПО, изменение конфигурационных параметров СКПП. При переключении в данный режим возможно влияние на функциональность и производительность СКПП.

2.1.4. Требования к производительности

При выполнении работ по развитию ГАИС «ЭРА-ГЛОНАСС» – СКПП должна

учитывать прогноз по нагрузке, указанный в Таблице 1.

Таблица 1.

Показатель	Значение
Способность формирования, УИР в год	не менее 12 млн.
Способность формирования, УИПП в год	не менее 240 млн.
Количество обрабатываемых запросов в секунду (кроме сервисных запросов, например, построение и вывод отчетов)	не менее 1000

2.1.5. Требования по сохранности информации и надежности системы

СКПП должна обеспечивать корректную обработку ситуаций, вызванных неверным форматом или недопустимыми значениями входных данных (форматно-логический контроль). В указанных ситуациях СКПП должна возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных, и обеспечивать целостность и сохранность данных СКПП.

Требования к процедурам резервного копирования и восстановления данных должны быть определены в эксплуатационной документации на СКПП.

Все требования к надежности СКПП необходимо учитывать в совокупности с требованиями проектной и эксплуатационной документации в части аппаратного обеспечения, необходимого для эксплуатации СКПП. СКПП должна сохранять во времени в установленных пределах значение комплексного показателя надежности – коэффициента готовности СКПП, характеризующего способность выполнять требуемые функции в заданных условиях, включая восстанавливаемость, наличие средств выявления ошибок.

Коэффициент готовности (минимальное значение показателя) – 0,99.

В СКПП должен обеспечиваться необходимый уровень защиты и сохранности информационных ресурсов в случаях:

- 1) непредвиденных сбоев и отказов программных и технических средств, включая сбой электропитания;
- 2) полного или частичного выхода из строя серверов, который влечет за собой потерю доступа к важной информации;
- 3) отказа оборудования СКПП резервного копирования;
- 4) отказа СКПП в результате ошибок персонала или пользователей СКПП.

Надежность СКПП должна обеспечиваться комплексом организационно-технических мер, в том числе:

- 1) резервированием отдельных компонентов СКПП (резервирование функций);
- 2) использованием средств резервного копирования СКПП;
- 3) диагностикой и мониторингом ошибок с помощью программных средств контроля (протоколирование событий функционирования подсистем);
- 4) диагностикой сбоев и отказов оборудования средствами СКПП

(мониторинг инфраструктуры);

5) защитой технических средств по электропитанию путем использования источников бесперебойного питания.

СКПП должна обеспечить следующие показатели надежности:

- время восстановления работоспособного состояния: не более 8 рабочих часов;
- резервное копирование данных производится один раз в 24 астрономических часа.

Для СКПП должны быть определены следующие требования к надежности в зависимости от категории аварийной ситуации, указанные в Таблице 2.

Таблица 2.

Аварийная ситуация	Показатель надежности	Целевое значение показателя	Механизм обеспечения надежности
Сбой питания на площадке размещения СКПП	коэффициент готовности	>0,99	Резервирование электропитания
Сбой в работе аппаратных средств и инфраструктурных сервисов СКПП	коэффициент готовности	>0,99	Резервирование
Сбой в работе общесистемного или специального ПО	коэффициент готовности	>0,99	Резервирование
Сбой в работе каналов связи	коэффициент готовности	>0,99	Резервирование канала связи
Сбой в работе СУБД	коэффициент готовности	>0,99	Резервное копирование
Сбой в работе прикладных сервисов	коэффициент готовности	>0,99	Резервирование

Показатель надежности СКПП – коэффициент готовности – должен быть рассчитан как отношение времени штатного функционирования к общему времени работы. Где общее время работы СКПП должно составлять 24 часа в сутки, 365 (366) дней в году, а время штатного функционирования включает в себя как время нахождения СКПП в штатном режиме функционирования, так и сервисные, технологические перерывы во время сервисного режима функционирования СКПП.

2.1.6. Требования по диагностированию СКПП

Диагностирование СКПП должно осуществляться непрерывно в автоматическом режиме.

Диагностирование должно осуществляться путем анализа записей в системных журналах СУБД, web-сервера и операционной системы, а также с помощью встроенных средств диагностирования ПО СКПП.

Диагностированию подлежат:

- случаи аварийных остановок и самопроизвольной перезагрузки ПО;
- случаи нарушений целостности базы данных и файловой системы;
- сбои при обращении к внешним информационным системам;
- сбои при выполнении регламентных операций резервного копирования.

СКПП должна обеспечивать диагностику своей работоспособности путем передачи журналов и метрик в централизованную систему диагностики АО «ГЛОНАСС».

СКПП и ее компоненты должны обеспечивать диагностику своей работоспособности путем передачи журналов и метрик в централизованную систему диагностики АО «ГЛОНАСС». Передаваемой информации должно быть достаточно для однозначной локализации уже произошедших ошибок или потенциальных проблем. Информация, поступающая от СКПП в централизованную систему диагностики АО «ГЛОНАСС», должна позволять однозначно указать элемент или группу элементов согласно спецификации развертывания, в которой произошли ошибки или в ближайшее время прогнозируются ошибки при нарушении установленных диапазонов значений для метрик мониторинга. Уровень логирования должен конфигурироваться и поддерживать, как минимум, следующие значения:

- DEBUG – логирование всех видов событий;
- INFO – логирование ошибок, предупреждений и сообщений;
- WARN – логирование ошибок и предупреждений;
- ERROR – логирование всех ошибок.

Для определенных уровней логирования должна быть возможность настроить передачу исчерпывающей информации обо всех действиях пользователей СКПП (внесение, изменение, удаление и т.п.) в отношении всех объектов данных, с которыми работает СКПП.

Обязательным набором метрик является:

- метрики использования системных ресурсов (CPU, RAM, Memory);
- время исполнения входящих запросов;
- количество успешных/неуспешных выполнений входящих запросов;
- время исполнения исходящих запросов или обращений;
- количество успешных/неуспешных выполнений исходящих запросов или обращений.

2.2. Требования к функциональным ролям пользователей СКПП

Функциональная роль означает набор возможных действий, которые выполняются пользователем в отношении СКПП.

СКПП должна обеспечивать поддержку ролевой модели и ролей пользователей, определенных в Таблице 3.

Таблица 3.

Роль	Функция
Пассажир	проверка рейса по уникальным идентификаторам
	передача в СКПП информации (обращения) о признаках и (или) фактах потенциальных нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами
Перевозчик	регистрация в СКПП (создание персонифицированной записи в СКПП)
	администрирование персонифицированной записи

Роль	Функция
	создание заявки на новый маршрут и передача в СКПП информации, необходимой для согласования нового маршрута
	создание и подача заявки на изменение действующего маршрута
	создание и подача заявки о прекращении действия свидетельства на маршрут
	передача в СКПП информации о перевозке пассажиров или иных лиц автобусами и о следовании автобусов без пассажиров, необходимой для формирования уникальных идентификаторов
	получение УИР
	внесение данных о заказных перевозках и перевозках для собственных нужд
	передача в СКПП информации о статусах выполнения перевозки пассажиров или иных лиц автобусами и о следовании автобусов без пассажиров
	делегирование владельцу ОТИ функций по получению уникальных идентификаторов и передача в СКПП информации о статусах выполнения перевозки пассажиров или иных лиц автобусами и о следовании автобусов без пассажиров
	передача в СКПП информации (обращения) о признаках и (или) фактах потенциальных нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами
Ространснадзор	получение статистических данных мониторинга перевозок пассажиров и иных лиц автобусами и следовании автобусов без пассажиров
	автоматизированное формирование пакета материалов о выявляемых с помощью системы признаках нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами по установленным шаблонам
	получение и согласование заявки на новый маршрут
	получение и согласование заявки на изменение существующего маршрута
	получение заявок о прекращении действия маршрута
	получение и согласование заявки на регистрацию нового ОП
	получение и согласование заявки на изменение данных о действующем ОП
	получение заявок о исключение ОП из реестра
	запрос и получение отчетности

Роль	Функция
Смежная информационная система	информационное взаимодействие с СКПП в соответствии и объеме, определенным отдельными соглашениями и (или) регламентами об информационном взаимодействии
Оператор СКПП	управление персонифицированными записями и доступом пользователей к СКПП
	анализ признаков и (или) фактов нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами, обращений пользователей и подготовка материалов для передачи в Ространснадзор
	управление взаиморасчетами с пользователями СКПП
	просмотр и изменение данных в СКПП по зарегистрированным обращениям в службе информационно-технической поддержки оператора
	формирование отчетности
	просмотр журнала действий пользователей и управление доступом к СКПП
Наблюдатель	передача в СКПП информации (обращения) о признаках и (или) фактах потенциальных нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами
	получение информации по рейсу по уникальному идентификатору
Владелец ОТИ	создание заявки на регистрацию нового ОП
	создание заявки на изменение данных о действующем ОП
	согласование пролегающих маршрутов
	создание заявки на исключение ОП из реестра
	получение УИР и УИПП (по поручению перевозчика)
	передача в СКПП информации о статусах выполнения перевозки пассажиров или иных лиц автобусами и о следовании автобусов без пассажиров (по поручению перевозчика)
	передача в СКПП информации (обращения) о признаках и (или) фактах потенциальных нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами
	получение информации по рейсу по уникальному идентификатору
ФБУ «Росавтотранс»	согласование заявки на новый маршрут
	согласование заявки на изменение существующего маршрута
	обработка заявок о прекращении действия маршрута

Роль	Функция
	согласование заявки на регистрацию нового ОП
	согласование заявки на изменение данных о действующем ОП
	обработка заявок о исключение ОП из реестра
	создание от лица перевозчика заявки на новый маршрут
	создание от лица перевозчика заявки на изменение существующего маршрута
	создание от лица перевозчика заявок о прекращении действия маршрута
	запрос и получение отчетности по пакетам материалов о выявляемых с помощью СКПП признаках нарушений в сфере осуществления перевозок пассажиров и иных лиц автобусами по установленным шаблонам
РОИВ	согласование заявки на новый межрегиональный маршрут
	согласование заявки на изменение существующего межрегионального маршрута
	согласование заявки на регистрацию нового ОП
	согласование заявки на изменение данных о действующем ОП
	создание вариантов путей подъезда к ОП с применением картографического сервиса
	подача заявления от органа исполнительной власти в интересах владельца ОП на регистрацию
	формирование отчетности
ФОИВ	просмотр сводной профильной аналитической информации
	формирование отчетности

2.2.1. Требования к объектной модели СКПП

СКПП должна обеспечивать поддержку объектной модели данных. Для всех информационных объектов СКПП должна обеспечивать их классификацию и возможность изменения состояний во времени.

К объектам СКПП должны относиться (как минимум, но не ограничиваясь) следующие сущности:

- 1) Рейс;
- 2) Перевозчик;
- 3) Транспортное средство;
- 4) Тип/вид ТС;
- 5) УИП;

- 6) УИМ;
- 7) УИПП;
- 8) УИР;
- 9) Перевозочный документ;
- 10) Остановочный пункт;
- 11) Маршрут;
- 12) Свидетельство на маршрут;
- 13) Карта маршрута;
- 14) Вариант маршрута;
- 15) Вариант расписания;
- 16) Модель навигационного оборудования и (или) IMEI навигационного оборудования (при необходимости);
- 17) Договор на оказание услуг оператором СКПП;
- 18) Персоналифицированная запись;
- 19) Начисление;
- 20) Платеж;
- 21) Роль;
- 22) Владелец (оператор) смежной информационной СКПП;
- 23) Правило выявления признака и (или) факта нарушения в сфере осуществления перевозок пассажиров и иных лиц автобусами;
- 24) Событие о выявлении признака и (или) факта нарушения в сфере осуществления перевозок пассажиров и иных лиц автобусами;
- 25) Отчет;
- 26) Событие;

2.2.2. Требования к функциям модулей СКПП

Функциональная архитектура СКПП должна состоять из подсистем и компонентов, указанных в Таблице 4.

Таблица 4.

Наименование модуля	Назначение модуля
Модуль информирования и доступа к информационным ресурсам	Доступ к информационным ресурсам и сервисам СКПП посредством графического интерфейса пользователя и шлюза доступа, консолидация информации, оповещение пользователей, ведение личных кабинетов пользователей
Модуль управления остановочными пунктами	Работа с данными об ОП
Модуль управления маршрутами	Работа с данными о маршрутах
Модуль поддержания процессов мониторинга перевозок	Работа с УИР и УИПП. Мониторинг и поддержка процессов управления рейсами, маршрутами
Модуль аналитики по выявлению признаков и (или) фактов нарушений законодательства при осуществлении	Автоматизация выявления различными способами признаков и (или) фактов нарушений в сфере осуществления перевозок пассажиров и иных лиц

перевозок	автобусами
Модуль управления взаимоотношениями с пользователями	Автоматизация процессов деятельности по работе с пользователями (управление договорами, заявками, обращениями, регистрацией и информированием)
Модуль управления отчетностью	Информационная и аналитическая поддержка деятельности пользователей, формирование и визуализация представления информации в текстовом и графическом видах в соответствии с ролевой моделью доступа
Модуль хранения и управления данными	Хранение и управление информационными объектами СКПП, обеспечение целостности данных, обеспечение доступа к данным
Модуль обеспечения информационной безопасности	Управление правами доступа, аутентификация и авторизация, обеспечение конфиденциальности, целостности и доступности данных
Модуль администрирования и журналирования	Журналирование, администрирование настроек СКПП
Модуль взаимодействия со смежными системами	Прием, передача, предварительная обработка, контроль и оперативное хранение данных взаимодействия со смежными информационными системами посредством программного интерфейса
«Народный контроль»	СКПП регистрации и учета статуса обращений (жалоб) наблюдателей

2.2.3. Требования к стандартизации и унификации

При создании СКПП должна обеспечиваться совместимость программных и технических решений, использование нестандартных и недокументированных технологий, классификаторов не допускается.

Проектирование моделей текущего состояния и целевых бизнес-процессов СКПП должно осуществляться с использованием нотации для описания бизнес-процессов.

2.2.4. Требования к подключению смежных информационных систем

Подключение смежных информационных систем к СКПП допускается только при условии, что такие системы соответствуют требованиям информационной безопасности, установленным законодательством Российской Федерации для обработки соответствующей категории информации (включая персональные данные), и имеют реализованные меры защиты, актуальные для выявленных угроз.

Оператор СКПП вправе проводить оценку соответствия смежных систем установленным требованиям безопасности в порядке, определенном регламентами взаимодействия.

2.2.5. Порядок информационного взаимодействия

ФОИВ, уполномоченные на обеспечение проведения эксперимента в соответствии с пунктом 3 постановления Правительства Российской Федерации от 11.11.2025 № 1776 «О проведении эксперимента по обеспечению электронного взаимодействия участников процесса перевозок пассажиров автомобильным транспортом по межрегиональным маршрутам регулярных перевозок», участвуют в информационном взаимодействии посредством:

- получения отчетных материалов, формируемых АО «ГЛОНАСС» на регулярной основе;

- направления письменных запросов в АО «ГЛОНАСС» о представлении справочной, аналитической и иной информации о ходе и результатах эксперимента (при необходимости);

- единой системы межведомственного электронного взаимодействия в соответствии с постановлением Правительства Российской Федерации от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия».

Для целей подписания документов пользователями с использованием технологии мобильной электронной подписи «Госключ» СКПП взаимодействует с подсистемой «Единая цифровая платформа подписания и хранения документов» федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)».

Порядок подключения, обмена данными и взаимодействия между СКПП и смежными информационными системами участников эксперимента в части, не урегулированной нормативными правовыми актами Российской Федерации, определяется отдельными регламентами информационного взаимодействия.

Регламенты информационного взаимодействия утверждаются оператором СКПП и являются неотъемлемой частью соглашения об информационном взаимодействии между операторами взаимодействующих систем.

В регламентах информационного взаимодействия должны быть конкретизированы:

- технические и программные интерфейсы (API) взаимодействия;
- форматы и структура передаваемых данных;
- процедуры аутентификации и авторизации;
- протоколы обеспечения конфиденциальности и целостности передаваемой информации (включая использование средств криптографической защиты информации, сертифицированных ФСБ России);
- регламентные процедуры, периодичность обмена;
- процедуры реагирования на инциденты и сбои при взаимодействии;
- ответственность сторон.

2.3. Требования к информационной безопасности и защите информации

2.3.1. Описание объекта защиты

На основании основных предварительных характеристик СКПП определены предварительные исходные данные, которые должны быть учтены при построении системы защиты информации.

В рамках эксперимента к СКПП не предъявляются требования в части обеспечения безопасности для государственных информационных систем

и критической информационной инфраструктуры.

СКПП является информационной системой персональных данных (далее – ИСПДн).

СКПП не является информационной системой общего пользования. Требования приказа ФСБ России № 416, ФСТЭК России № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» не применимы.

Для СКПП необходимо обеспечение третьего уровня защищенности персональных данных (УЗЗ), при их обработке в ИСПДн, в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Реализация требований по защите информации и обеспечению безопасности должна соответствовать нормативным требованиям ФСТЭК России и ФСБ России в части защиты ИСПДн.

Объектами защиты в СКПП являются:

- информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию и представленные на магнитных, оптических и других носителях;

- информация, содержащаяся в СКПП, остаточная информация на носителях информации, а также передаваемая по внутренним каналам связи, не выходящим за пределы контролируемой зоны СКПП:

- служебная информация (сведения ограниченного распространения);

- персональные данные;

- сведения, составляющие коммерческую тайну;

- технологическая информация;

- ключевая, аутентифицирующая и парольная информация;

- конфигурационная информация;

- управляющая информация;

- информация о структуре системы защиты информации СКПП;

- резервные копии файлов с конфиденциальной информацией;

- технические средства СКПП;

- телекоммуникационное оборудование;

- АРМ администраторов;

- серверное оборудование;

- система хранения данных;

- ПО;

- общесистемное ПО;

- прикладное ПО;

- специальное ПО;

- средства защиты информации;

- документация (техническая, эксплуатационная) на средства защиты информации и политики информационной безопасности СКПП.

Иная информация субъектов, обрабатываемых СКПП:

- 1) Обрабатываемые данные оператора СКПП:

- наименование организации;
- бухгалтерские данные (начисление и платежи по всем перевозчикам);
- статистические данные по перевозкам (количество УИР, УИПП, рейсов за период).

2) Обрабатываемые данные перевозчика:

- данные налогового учета (ОГРН, ИНН, наименование организации);
- данные по транспортному средству (ГРН, модель, наличие лицензии);
- данные о рейсах (маршрут, расписание, ТС, УИР);
- данные о перевозочных документах (номера перевозочных документов, количество УИПП).

3) Обрабатываемые данные владельца ОТИ:

- данные налогового учета (ОГРН, ИНН, наименование организации);
- данные об остановочных пунктах (наименование, координаты, др.).

Обрабатываемые данные ФОИВ, РОИВ, ФБУ «Росавтотранс»: наименование органа (организации).

СКПП актуальны угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и (или) прикладном ПО, используемом в информационной среде – угрозы 3-го типа.

К служебной технологической информации ограниченного распространения, обрабатываемой СКПП, относятся:

- данные, содержащиеся в эксплуатационной документации на компоненты и систему защиты СКПП;
- содержимое конфигурационных файлов сетевого оборудования, технических и программных средств СКПП, СрЗИ;
- содержимое регистрационных записей системного, специального и прикладном ПО СКПП;
- содержание регистрационных записей сетевого оборудования, технических и программных средств СКПП, СрЗИ.

Обработка информации в СКПП осуществляется в соответствии с требованиями:

- Федерального закона от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства Российской Федерации от 01.12.2021 № 2152 «Об утверждении Правил создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;
- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»;

– приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказа ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

СКПП не предназначена для обработки информации, содержащей сведения, составляющие государственную тайну и информации с пометкой «ДСП» («Для служебного пользования»).

Программные и программно-аппаратные СрЗИ, входящие в состав СКПП, должны быть сертифицированы в системе сертификации ФСТЭК России. Применяемые СрЗИ должны соответствовать следующим требованиям:

- 5 или более высокому уровню доверия;
- средствам защиты информации не ниже 5 класса;
- средствам вычислительной техники не ниже 5 класса.

Программные и программно-аппаратные средства криптографической защиты информации, входящие в состав СКПП, должны быть сертифицированы в системе сертификации ФСБ России класса не ниже КС2.

Для подписания документов пользователями СКПП с использованием технологии мобильной электронной подписи «Госключ» используются средства электронной подписи класса КС1.

2.3.2. Общие требования к информационной безопасности и защите информации

Защита информации СКПП должна реализовывать меры защиты информации в соответствии с требованиями приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для реализации 3 уровня защищенности персональных данных, в том числе направленные на нейтрализацию актуальных угроз безопасности информации.

Организационные и технические меры защиты информации, реализуемые в СКПП, должны быть направлены на исключение неправомерных:

- доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- уничтожения или модифицирования информации (обеспечение целостности информации);
- блокирования информации (обеспечение доступности информации).

Модель угроз и нарушителя информационной безопасности СКПП подлежит разработке путем адаптации типовой модели угроз и нарушителя безопасности

информации для СКПП, и должна содержать описание СКПП и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации, с учетом требований установленных в:

- приказе ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- методическом документе «Методика оценки угроз безопасности информации», утвержденном ФСТЭК России 05.02.2021;

- методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденных ФСБ России 31.03.2015 № 149/7/2/6-432.

2.3.3. Общие требования по разработке безопасного программного обеспечения

В процессе моделирования угроз безопасности информации должны быть рассмотрены угрозы безопасности информации, которые могут возникать в процессах разработки и использования ПО. Все выявленные угрозы должны быть описаны и включены в Модель угроз безопасности информации СКПП. Для формирования перечня и описания угроз безопасности информации, которые могут возникать в процессах разработки ПО, следует использовать ГОСТ Р 58412 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения» (утвержден и введен в действие приказом Росстандарта от 21.05.2019 № 204-ст).

Для формирования перечня и описания угроз безопасности информации, которые могут возникать при использовании ПО в составе СКПП, должны использоваться:

- сведения о предполагаемых компонентах программы;
- сведения об интерфейсах компонентов программ;
- сведения о предполагаемых алгоритмах, методах и протоколах взаимодействия компонентов программы;
- сведения о вариантах и методах конфигурирования программы, ее компонентов, а также планируемой среды функционирования ПО;
- информацию о заимствованных компонентах сторонних разработчиков;
- информацию из банка данных угроз безопасности информации ФСТЭК России (<https://bdu.fstec.ru>).

Для каждого используемого при разработке СКПП инструментального средства должна быть определена и зафиксирована в проектной документации следующая информация:

- наименование и идентификационные признаки инструментального средства;
- наименование разработчика инструментального средства;
- ссылка на эксплуатационные документы инструментального средства;
- значения применяемых при создании программы конфигураций инструментального средства.

При разработке СКПП возможно использовать заимствованные компоненты сторонних разработчиков (библиотеки, фреймворки, интерпретируемые скрипты и др.) только при наличии исходного кода таких компонентов.

В рамках проводимых работ по разработке ПО должны проводиться инструментальные исследования в отношении разрабатываемого ПО на предмет выявления недостатков и уязвимостей в ПО.

Результаты проведенных инструментальных исследований должны быть отражены в соответствующих протоколах исследований ПО. Все выявленные и подтвержденные уязвимости и недостатки ПО критического и высокого уровня влияния необходимо устранить до момента перевода СКПП в опытную эксплуатацию.

В процессе разработки ПО применяются технические и организационные меры, обеспечивающие регистрацию всех событий, связанных с фактами изменения элементов конфигурации, в журналах регистрации событий.

2.3.4. Требования к реализации системы информационной безопасности

СКПП создается в соответствии с нормами и требованиями «ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утвержден и введен в действие приказом Росстандарта от 24.10.2024 № 1504-ст).

СКПП должна обеспечивать функционирование в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Система защиты информации должна обеспечивать реализацию мер защиты информации в соответствии с приказами ФСТЭК России:

- от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (действует до 01.03.2026);

- 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» (вступает в силу с 01.03.2026).

В СКПП предусмотрены средства защиты от несанкционированного доступа к информации, разрушения информации, в том числе путем доступа через графические и/или программные интерфейсы СКПП, внешние носители информации, корпоративные компьютерные сети оператора СКПП, а также физический доступ к техническим средствам СКПП.

Возможность прямого внесения изменений в информационные базы данных

СКПП должна быть исключена.

У оператора СКПП не должно быть технической возможности получать информацию о паролях учетных записей пользователей (хранение паролей в СКПП обеспечивается в зашифрованном виде).

2.3.5. Требования к автоматизированным рабочим местам

АРМ пользователей СКПП (включая привилегированных), размещенные на пользовательских площадках (пользовательский (клиентский) сегмент СКПП), по умолчанию рассматриваются как внешние информационные системы. В отношении указанных АРМ должна быть реализована мера защиты информации УПД (управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы))

Правила и процедуры защиты АРМ должны устанавливаться в соответствующих организационно-распорядительных документах по защите информации в СКПП. Описание архитектуры СКПП на инфраструктуре АО «ГЛОНАСС» в части взаимодействия АРМ и серверного сегмента должно отражаться в модели угроз и нарушителя, а также иных документах создаваемой СКПП.

2.3.6. Требования об обеспечении защиты информации в ходе эксплуатации/выводе из эксплуатации СКПП

В соответствии с законодательством Российской Федерации в области обеспечения безопасности информационных систем, оператор СКПП обязан организовать надлежащую защиту обрабатываемой в СКПП информации на протяжении всего жизненного цикла СКПП.

На этапе эксплуатации СКПП оператор должен выполнять следующие мероприятия:

- обеспечивать функционирование системы защиты информации СКПП в соответствии с эксплуатационной документацией;
- регулярно анализировать угрозы информационной безопасности и выполнять мероприятия по устранению уязвимостей;
- контролировать эффективность мер защиты информации;
- проводить мероприятия, по периодической оценке, уровня защищенности не реже одного раза в полгода;
- проводить мероприятия по практической отработке действий сотрудников структурного подразделения, обеспечивающего информационную безопасность СКПП по реагированию на компьютерные инциденты, атаки и вторжения не реже, чем раз в 3 месяца, при участии не менее 80% сотрудников структурного подразделения «АО «ГЛОНАСС», обеспечивающего информационную безопасность.

Для обеспечения надлежащего уровня информационной безопасности СКПП необходимо регулярно проводить мероприятия по оценке их класса защищенности. Эти мероприятия включают в себя комплекс организационных и технических мер, направленных на выявление потенциальных уязвимостей, оценку рисков и определение соответствия СКПП установленным требованиям безопасности.

В целях своевременного выявления изменений в конфигурации СКПП, появление новых угроз и уязвимостей, а также контроля эффективности

применяемых мер защиты периодичность проведения мероприятий по оценке уровня защищенности СКПП должна составлять не менее одного раза в шесть месяцев.

В целях обеспечения эффективной защиты информации в СКПП в процессе ее эксплуатации необходимо регулярно проводить практическую отработку действий сотрудников структурного подразделения АО «ГЛОНАСС», ответственного за информационную безопасность СКПП. Эти мероприятия должны быть направлены на отработку навыков своевременного обнаружения, анализа и реагирования на потенциальные компьютерные инциденты, атаки и попытки несанкционированного доступа к ресурсам СКПП.

При подготовке СКПП к выводу из эксплуатации или принятии решения о прекращении обработки информации оператор обязан обеспечить:

- комплексное завершение обработки и передачи информации в соответствии с установленным порядком;
- выполнение процедур по обеспечению информационной безопасности в условиях прекращения функционирования СКПП;
- физическое уничтожение носителей информации в случае необходимости.