

Т-АВИАС

Цифровая платформа
управления беспилотным
транспортом: обеспечение
безопасности информации

Толпыгин А.С.

к.т.н., главный конструктор

«ЦИФРОПОЛ-2025»



Научно-практическая
специальная конференция

Меры государственной поддержки беспилотного транспорта

Постановление Правительства РФ от 9.03.2022 № 309 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств».

Постановление Правительства РФ от 26 ноября 2018 г. № 1415 «О проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств».

План мероприятий («дорожная карта») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Автонет», утвержденный распоряжением Правительства Российской Федерации от 29 марта 2018 г. № 535-р.

Стратегия развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года, утвержденная постановлением Правительства Российской Федерации от 21 июня 2023 г. № 1630-р.

Емкость рынка (до 2030)*

SOM: 75 млрд. руб.

SAM: 350 млрд. руб.

TAM: 1,5 трлн. руб. (в России запланированы государственные инвестиции в 1 трлн. руб. в отрасль БАС)

PAM: 5,6 трлн. руб (БРИКС)

В России в 2027 г.*

100+ тыс.
беспилотных автомобилей

2+ млн.
беспилотных летательных аппаратов

*по данным [AERONEXT](#), Gartner, ГАЗ, Камаз и Сбравтотех

SOM – реально достижимый объем рынка
SAM – доступный объем рынка
TAM – общий объем рынка
PAM – потенциальный объем рынка

Проблемы

Задачи контроля:

- полный контроль трафика в границах зон социальных объектов, защищаемых объектов критической инфраструктуры;
- киберустойчивость БТС и защиту от их неправомерного применения;
- контроль выполнения маршрутных (полетных) заданий. Выявление и предотвращение аномалий в поведении БТС;
- соответствие БТС законодательству РФ и требованиям регуляторов по безопасности их применения.

Потребители	Госорганы* 40+ Госпредприятия** 50+	Производители беспилотных авиасистем 50+	Производители беспилотных автомобилей 4	Эксплуатанты БТС >15 тыс.	Надзорные органы и разработчики средств борьбы с БПЛА
Проблемы	Бесконтрольное применение БТС: терроризм, шпионаж Интеграция БТС в единое пространство с пилотируемым транспортом Аварии и катастрофы в отсутствие данных о состоянии БТС и своевременной реакции	Перехват управления БТС Невозможно оформление сертификата летной годности и сертификатов безопасности БТС Риски снятия БТС с производства из-за растущих требований регуляторов в части безопасности	Перехват управления Бесследное исчезновение БТС и грузов, невыполнение полетного задания Постановка на учет - от 45 дней до первого полета с момента покупки	Отсутствие возможности остановки БТС в экстренных ситуациях	

* – Минцифры России, Минпромторг России, Минтранс России, МЧС, МВД, МО РФ и др.
** –Росавтодор, ГКУ ЦОДД, Росавиация, ОрВД и др.

БТС – беспилотные транспортные средства
БПЛА – беспилотные летательные аппараты

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ БЕСПИЛОТНОГО ТРАНСПОРТА

По методике просеивания угроз из [Банка данных угроз безопасности информации ФСТЭК России](#) могут быть осуществлены **30+ угроз** с высокой вероятностью и иметь уровень влияния высокий

Угрозы	Вер-ть	Влияние	Ранг	Последствия
УБИ.006: Угроза внедрения кода или данных	Выс.	Выс.	1	Перехват злоумышленником управления БТС: ■ блокировка движения на магистралях и улицах городов; ■ совершение противоправных действий с применением БТС, умышленные ДТП в том числе теракты; ■ совершение противоправных действий в отношении пассажиров БТС; ■ воровство грузов и самих БТС; ■ применение БТС в личных целях. Нарушение целостности информации передаваемой БТС в пункты управления: ■ нарушение работоспособности пунктов и центров управления БТС; ■ дезинформация о дорожной ситуации.
УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации	Выс.	Выс.	1	
УБИ.011: Угроза деавторизации санкционированного клиента беспроводной сети	Выс.	Выс.	1	
УБИ.023: Угроза изменения компонентов информационной (автоматизированной) системы	Выс.	Выс.	1	
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Выс.	Выс.	1	
УБИ.031: Угроза использования механизмов авторизации для повышения привилегий	Выс.	Выс.	1	
УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными	Выс.	Выс.	1	
УБИ.036: Угроза исследования механизмов работы программы	Выс.	Выс.	1	
УБИ.047: Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Выс.	Выс.	1	
УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Выс.	Выс.	1	
УБИ.069: Угроза неправомерных действий в каналах связи	Выс.	Выс.	1	
УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Выс.	Выс.	1	
УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	Выс.	Выс.	1	
УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи	Выс.	Выс.	1	

Типовые проблемные вопросы защиты информации в БТС

1. Отсутствуют перечни защищаемой информации и защищаемых информационных ресурсов

2. Отсутствуют или не проработаны модели угроз и нарушителей для БТС

3. Система защиты информации не проектировалась, защита информации в БТС решается стихийно

4. Не защищается информация в процессе разработки БТС

5. Методические и руководящие документы по защите информации в организации не внедрены

6. Аудит информационной безопасности никогда не проводился и(или) проводился фрагментарно

7. Для организации каналов связи с БТС используется LTE, не защищается

8. Защита ИТВ с БТС строится в лучшем случае на основе VPN

9. Не определены требования по защищенности от НСД, уровню контроля НДВ, принадлежности к КИИ, ПДн и др.

10. Внутренняя сенсорная сеть БТС не защищена. И даже не предполагается ее защита

11. Не доверенная элементная база: процессоры, материнские платы, программируемые контроллеры

12. Не проработаны вопросы противодействия средствам РЭБ, не решены вопросы РЭС

13. Лицензии на ведение каких-либо видов деятельности по защите информации отсутствуют

14. Вопросы применения СКЗИ не проработаны

РЕШЕНИЕ

Цифровая платформа контроля и управления движением БТС со встроенными средствами ЗИ

Потребность государства – создать распределенную защищенную автоматизированную систему контроля и управления движением беспилотных транспортных средств (АСКУД БТС).

Цель – разработать инструментарий для создания типовых центров контроля и управления движением беспилотных транспортных средств, обеспечивающий безопасность информации

Задачи:

- Разработать интеллектуальную информационно-управляющую платформу ИИТ для беспилотных транспортных средств (далее – Цифровая платформа БТС)
- Анализ факторов угроз информационной и кибербезопасности БТС и разработать систему моделей угроз и нарушителей информационной и кибербезопасности БТС.
- Разработка общей и частных моделей по видам транспорта: автомобильный, железнодорожный, морской, речной, воздушный.
- Выработка мер (разработка рекомендаций) защиты от угроз информационной и кибербезопасности БТС.
- Обеспечить безопасное информационно-техническое взаимодействие БТС с центрами управления и между собой.
- Разработать и ввести в действие необходимую нормативно-методическую документацию в области информационной и кибербезопасности БТС.

Организация сети ЦКУ БАС

Уровни реализации функций ЦКУ БАС

Элементы сети Центров контроля и управления движением

Главный центр контроля и управления (федеральный уровень)

Функционал:

- планирование заданий для региональных центров управления
- выдача заданий региональным центрам управления
- получение от региональных центров сообщений о статусе выполнения заданий, контроль и учет выполнения заданий
- оптимизация распределения заданий между региональными центрами управления

Росавиация (ОрВД) + интеграция с
Ситуационным центром МВД РФ,
НЦУО РФ, НЦУКС МЧС РФ,

Центры контроля и управления (региональный/ведомственный уровень)

Функционал:

- получение и обработка заданий от вышестоящего центра управления
- возможность принятия на себя роли вышестоящего центра
- выдача заданий центрам управления мобильного уровня
- контроль за выполнением заданий центром управления мобильного уровня
- предоставление вышестоящему центру управления информации о ходе выполнения поставленных задач

ФОИВ,
РОИВ

Подвижные (мобильные) центры контроля и управления (региональный уровень)

Функционал:

- получение заданий от вышестоящего центра управления
- возможность автономного функционирования и принятия на себя роли вышестоящего центра
- распределение заданий между БВС и их выдача
- контроль за исполнением заданий
- предоставление отчетов о ходе выполнения заданий вышестоящему центру управления



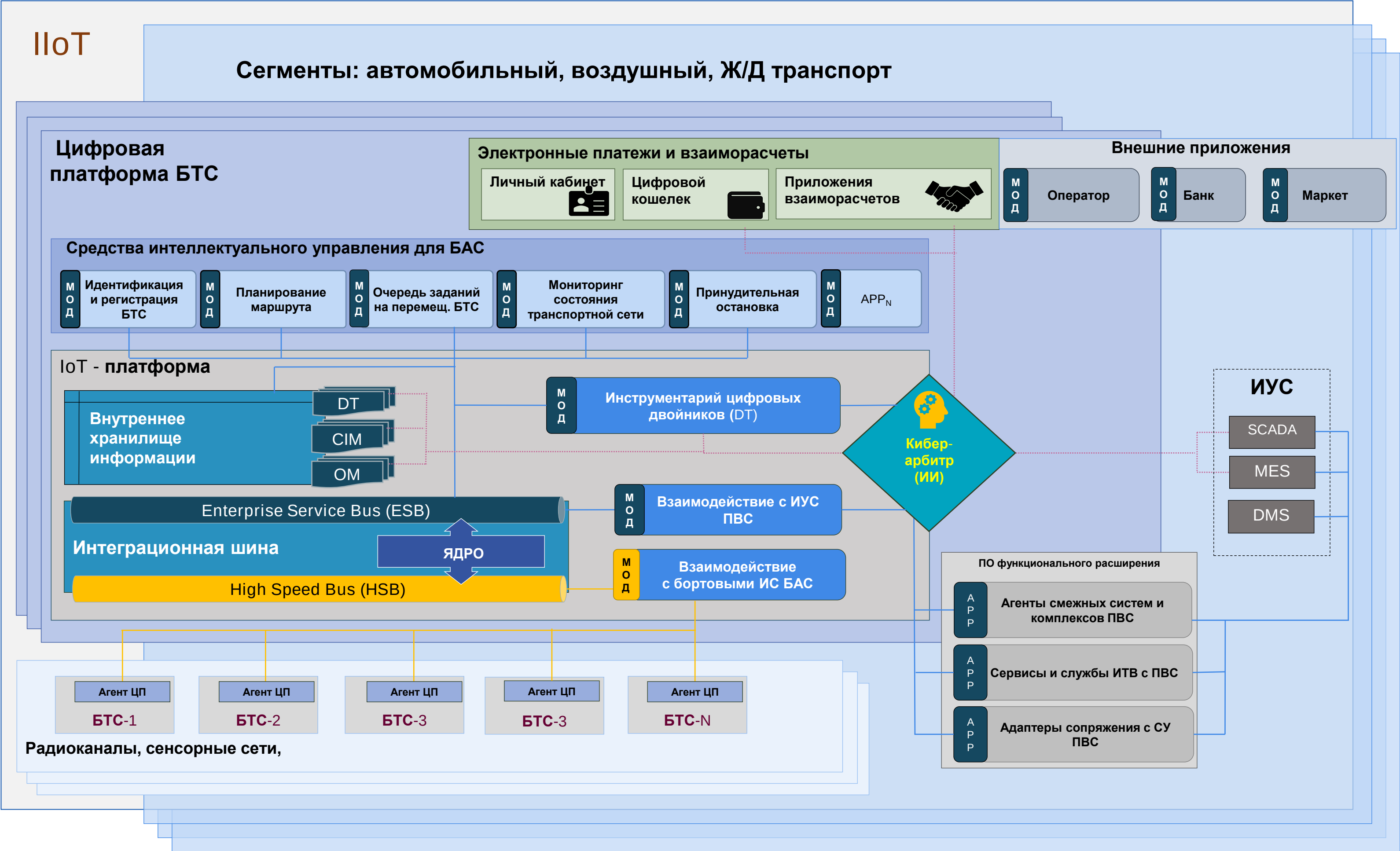
Система моделей угроз

8

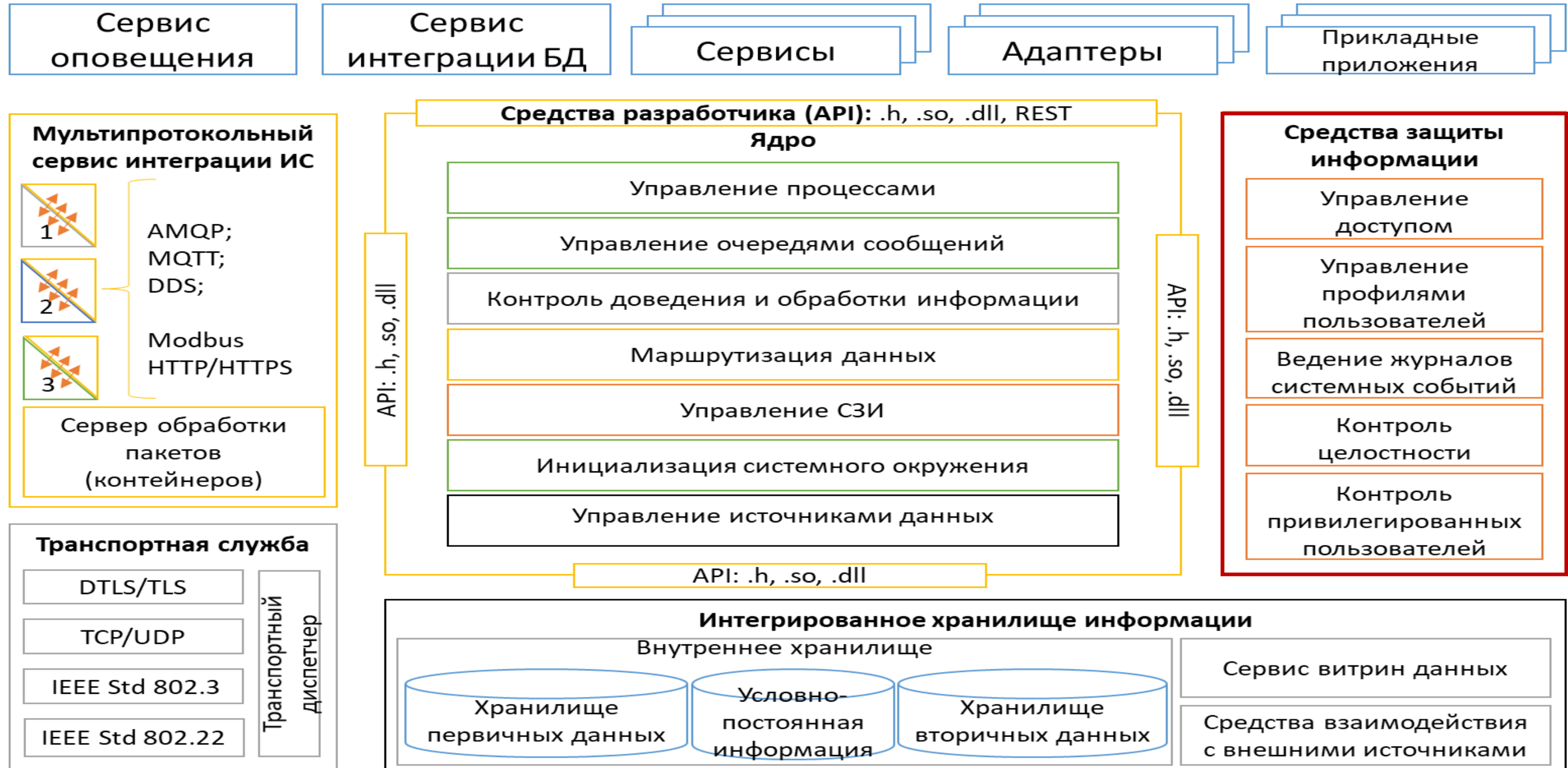


СЛ – сверхлегкий (до 4 кг); Л – легкий (4-30 кг); С – средний (30-500 кг); Т – тяжелый (свыше 500 кг);
типы БАС: С – самолетный, В – вертолетный, М – мультироторный, К – конвертоплан, Г – гибридный.

Архитектура цифровой платформы БТС



Структурно-функциональная схема ядра IoT-платформы в составе Цифровой платформы БТС



Статус развития технологий и продуктов в составе цифровой платформы

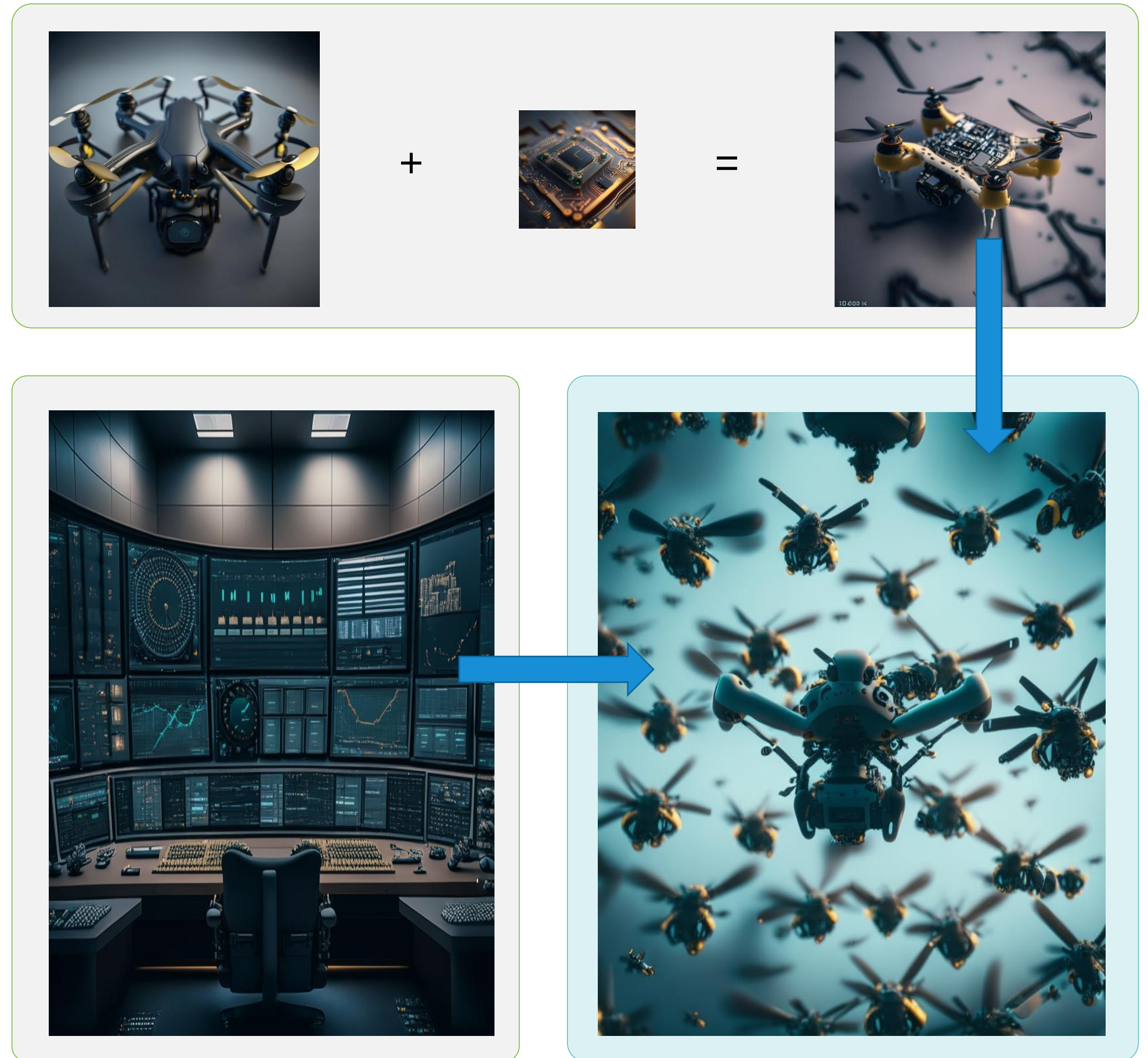
Технологии, продукты	Статус
Интеграционная шина ▪Enterprise Service BUS. Технологическая платформа интеграции приложений ▪High Speed BUS. Технологическая платформа для взаимодействия с терминальными устройствами в режиме реального времени ▪Служба гарантированной доставки данных и контроля обработки данных на принимающей стороне	PRO
Система операционного управления ▪Служба управления распределенной вычислительной инфраструктурой ▪Служба мониторинга бизнес-процессов	MVP
Конструктор цифровых двойников технических объектов и бизнес-процессов	ADV TECH
Система интеллектуального управления бизнес-процессами ▪Очередь заданий на перемещение БТС ▪Монитор состояния транспортной сети ▪Построение карты погоды ▪Выработка рекомендаций скоростного режима ▪Расчет мультимодальных поездок	TECH
Интегрированное хранилище информации и объединенный коммуникационный центр консолидации данных от разнородных источников	ADV TECH
Агентство доступа к первичным сетям передачи данных	ADV TECH
Интерактивный экспресс-анализ данных ▪Служба экспресс-анализа серий данных	TECH



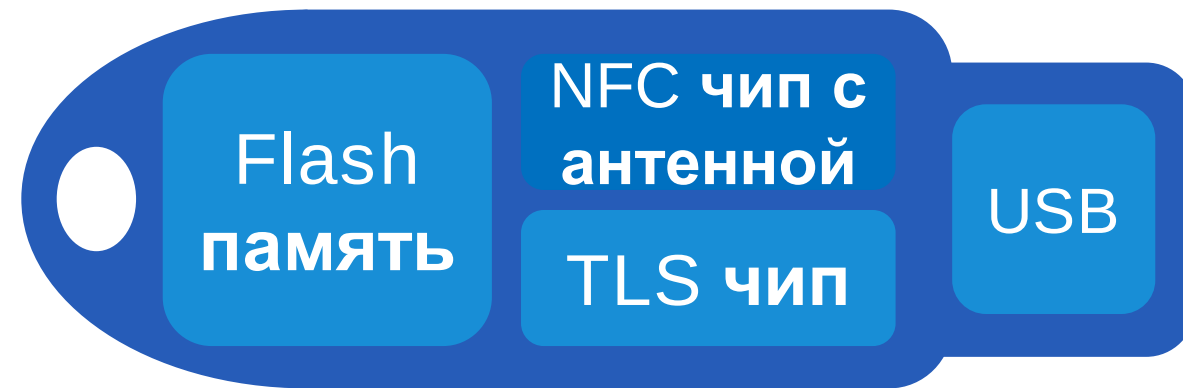
РЕШЕНИЕ (ТЕХНОЛОГИЯ)

Предлагается встраиваемое решение – инъекция «мозжечка» в систему управления БТС, которое обеспечит:

- Полный контроль обстановки возле защищаемых объектов критической инфраструктуры
- Киберустойчивость беспилотных транспортных средств (БТС) и защита от неправомерного применения
- Контроль выполнения маршрутного задания.
Выявление и предотвращение аномалий в поведении БТС
- Соответствие БТС законодательству РФ и требованиям регуляторов по безопасности их применения



Технология DroneCerebellum



Замысел



Реализация
прототипа

Технология DroneCerebellum в основе Цифровой платформы позволит обеспечить контроль и управление беспилотниками из Центра мониторинга за счет инъекции «мозжечка» в их систему управления. Также DroneCerebellum обеспечит защиту каналов взаимодействия беспилотников с пунктами контроля и управления от перехвата управления.

ППРФ от 30.11.2024 № 1701

«Об утверждении требований к оснащению пилотируемых воздушных судов и БАС оборудованием связи, навигации, наблюдения, автоматического предотвращения столкновений, к оснащению БАС оборудованием удаленной идентификации и оборудованием линий управления беспилотными авиационными системами и контроля БАС, средствами криптографической защиты информации, сертифицированными в соответствии с требованиями ФОИВ в области обеспечения безопасности, и Правил оснащения пилотируемых воздушных судов и БАС оборудованием, предусмотренным пунктом 1 статьи 78.3 ВЗК РФ»

Предложение

- Создать ПАК ОИБ ОКИИ – унифицированный модульный программно-аппаратный комплекс, включающий ВСЕ необходимые средства защиты, соответствующие требованиям ФСТЭК России
- ПАК конфигурируется для любой категории объекта КИИ
- Все элементы ПАК интегрированы в единую систему, проверены на совместимость и бесконфликтность
- В составе ПАК исключительно отечественные программно-аппаратные средства защиты

Архитектура систем ИБ (to be)



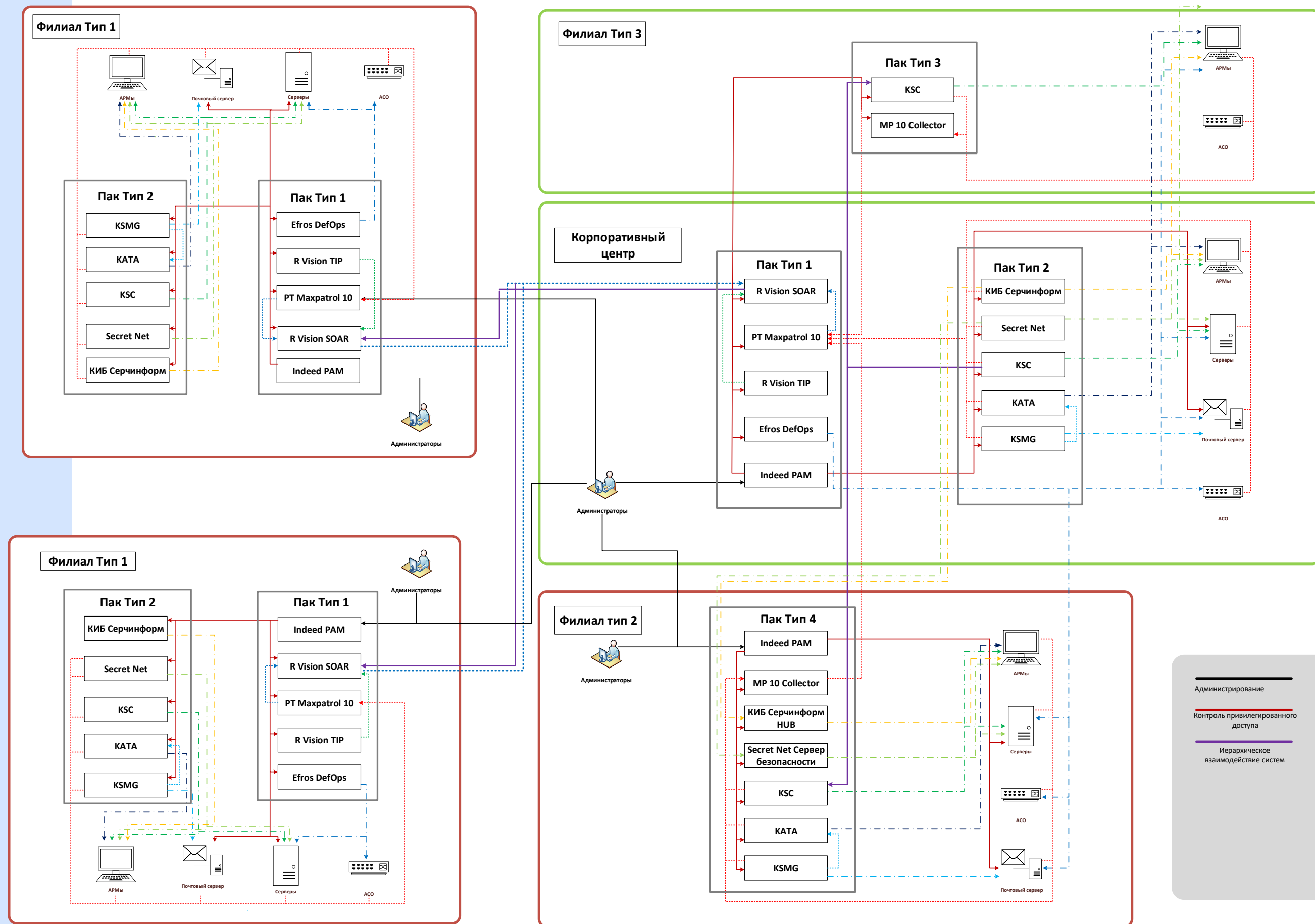
Состав ПАК

ПАК ОИБ ОКИИ – модульный программно-аппаратный комплекс, имеющий в составе ВСЕ средства защиты, соответствующие требованиям ФСТЭК России, предъявляемым к той или иной категории объекта КИИ, интегрированные в единую систему и функционирующие на отечественных программно-аппаратных решениях.

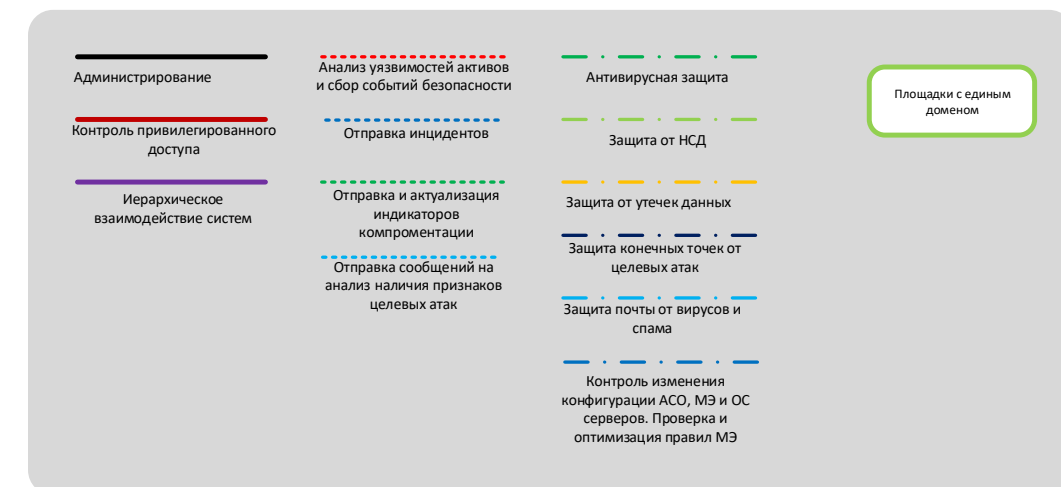
Аппаратная часть	Программная часть	Стэк
Отечественные: серверное оборудование, маршрутизаторы и системы хранения данных	SOAR/SGR	SVision/RVision
	SIEM	MaxPatrol SIEM/KUMA
	DLP	InfoWatch/SearchInform
	Антивирусное ПО	Касперский (KATA, KEDR, AV)
	СЗ от НСД	Код безопасности
	Средства межсетевого экранирования	Код безопасности, UserGate
	NGFW	PT, UserGate, Ростелеком
	Защита АСУТП	PT ISIM, Kaspersky ICS
Иные средства защиты, например: DECAP, IDM, PAM, решения однонаправленной передачи данных (USB, диод). Отечественные среды виртуализации, операционные системы, СУБД.		

В состав ПАК войдут программные и аппаратные средства исключительно отечественных производителей и разработчиков

Типовая схема реализации СОИБ на ПАК ОИБ ОКИИ



В состав ПАК войдут программные и аппаратные средства исключительно отечественных производителей и разработчиков



Что есть и что делать?

Имеем

Наименование	Описание
Собранный и эксплуатируемый ПАК	В ПАО «Ил» функционирует ПАК на базе иностранного аппаратного оборудования и операционных систем
Проект на создание	Проектная документация на систему включает в себя Техническое задание, частные технические задания на подсистемы, проектное решение и эксплуатационную документацию
Сертификация ФСТЭК России	Все используемые средства защиты имеют соответствующие сертификаты ФСТЭК России и ФСБ России На ПАО «Ил» имеется лицензия ФСТЭК России по технической защите конфиденциальной информации
Компетенции	На ПАО «Ил» в штате имеются высококвалифицированные специалисты обеспечивающие весь комплекс работ от создания комплекса, до его настройки и эксплуатации на протяжении 6 лет

Делаем

Задача	Результат
Создать стенд ПАК ОИБ ОКТИ	Готовый стенд
Компетенции	Усилить имеющуюся команду специалистами. Обеспечить трансфер и развитие имеющихся компетенций. Увеличить имеющийся ресурс
Провести тестирование на объекте промышленности ПАО «Ил	Рабочий опытно-промышленный образец эксплуатируемый предприятием ОПК
Сертификация ФСТЭК России	Документ, подтверждающий факт соответствия ПАК требованиям ФСТЭК России
Обеспечить финансирование установки ПАК на предприятия ОПК за счет ФЦП	Сформировать и утвердить ФЦП
Реализация программы на предприятиях	На всех предприятиях-субъектах КИИ установлен ПАК ОИБ ОКТИ

Организация и управление

Схема взаимодействия при обеспечении информационной безопасности объектов критической информационной инфраструктуры РФ (ОКИИ) на предприятиях ОПК



Сертификация по требованиям регуляторов

ноя. 2022: ЗАО «НПЦ «ИРС» - сертифицирован ПК «Атлант-МР» в составе изделия 83т525МР в системе сертификации Минобороны России.
Сертификат соответствия №6040 выдан 8.11.2022 г.

дек. 2015: АО «РТИ» – Заключение Федерального органа по сертификации средств защиты информации на типовую защищенную Интеграционную платформу «КАПИТАН» от 19.11.2014 г. по обращению ОАО «РТИ» от 7.11.2014 г. исх.№ 807/РТИ-ЗД

авг.2010: [С сайта ФСТЭК России](#) (текст для поиска – БюрократЪ):

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство	Схема сертификации	Испытательная лаборатория	Орган по сертификации	Заявитель	Реквизиты заявителя (индекс, адрес, телефон)	Информация об окончании срока технической поддержки, полученная от заявителя
2152	10.08.2010	10.08.2019	система электронного документооборота «ИВК БюрократЪ™»	Соответствует требованиям документов: РД НДВ(2)	серия	АО «НПО «Эшелон»	ООО «ЦБИ»	АО «ИВК»	129110, г. Москва, ул. Гиляровского, д. 57, стр. 1, комн. 73, (495) 221-6580	10.08.2069

авг.2005: [С сайта ФСТЭК России](#) (текст для поиска – Юпитер):

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство	Схема сертификации	Испытательная лаборатория	Орган по сертификации	Заявитель	Реквизиты заявителя (индекс, адрес, телефон)	Информация об окончании срока технической поддержки, полученная от заявителя
894/1	01.08.2005	01.08.2020	унифицированные программные средства организации, контроля и управления вычислительным процессом в неоднородных вычислительных сетях «ИВК ЮПИТЕР», версии 5.0, (шифр изделия - ЛНКВ.12736-05)	Соответствует требованиям документов: РД НДВ(2), РД СВТ(3)	серия	АО «ЦБИ-сервис»	ФСТЭК России	АО «ИВК»	129110, г. Москва, ул. Гиляровского, д. 57, стр. 1, комн. 73, (495) 221-6580	01.08.2070

T-AVIAS

Российский разработчик программного обеспечения беспилотных авиационных систем

Компания специализируется на создании киберзащищенных систем контроля и управления беспилотного транспорта и роботизированных систем на базе платформы АТЛАНТ-БАС

Толпыгин Алексей Сергеевич

Тел.: +7(985)360-0423 E-mail: tas@tavias.ru

Резидент АНО «ФЦ БАС»

ФОНД НТИ Фонд поддержки проектов
Национальной технологической
инициативы

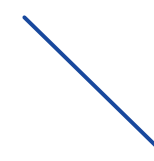
Резидент АНО «НПЦ БАС САМАРА»

НПЦ САМАРА
БЕСПИЛОТНЫЕ АВИАЦИОННЫЕ СИСТЕМЫ

Партнеры



ИВК ИНФОРМАЦИОННАЯ
ВНЕДРЕНЧЕСКАЯ
КОМПАНИЯ



Приложения

Некоторые практические аспекты

ПОТРЕБНОСТЬ В ТЕХНОЛОГИЧЕСКИХ И ИНЫХ ПАРТНЕРСТВАХ

Методы работы на целевых рынках, каналы продвижения

Участие в отраслевых
мероприятиях и выставках

Внедрение в учебный процесс в вузах
(МосУ МВД им. В.Я. Кикотя, Академия
государственной противопожарной службы
МЧС России, МГТУ им. Н.Э. Баумана и др.

Проведение рекламных компаний через
специализированные учебные центры
подготовки руководителей и сотрудников
организаций, отвечающих за
противопожарную безопасность

Публикации в журналах



Партнеры

- + ВНИИ ГОЧС (ФЦ)
МЧС России
- + СТиС МВД России
- + НИЦ Институт
им. Н. Е. Жуковского
- + ПАО Авиакомплекс
им. С.В. Ильюшина
- + ФЦ БАС
- + МГТУ
им. Н.Э. Баумана
- + Академия
государственной
противопожарной
службы МЧС России
- + ЗАО ИВК

ДРОН-ОХРАННИК

Дрон направляется к месту инцидента после получения сигнала от системы мониторинга.

С помощью камер идентифицируется цель и оценивается ситуация.

01 —

Активация электрошокера

Оператор удаленно подтверждает активацию электрошокера. Электрический разряд временно нейтрализует нарушителя.

02 —

Мониторинг ситуации

Дрон зависает над местом происшествия, продолжая мониторинг до прибытия охранников.



ДРОН-ПОЖАРНЫЙ

Система автоматически отправляет уведомление оператору и запускает ближайший готовый дрон

Дрон приближается к очагу возгорания или влетает в зону пожара и активирует огнетушащее средство

Тушение пожара

Система управления или оператор активирует механизм сброса огнетушащего средства

Мониторинг ситуации

После первичного тушения дрон продолжает мониторинг места возгорания



СРАВНЕНИЕ ДРОНА-ПОЖАРНОГО И ПОЖАРНЫХ СЛУЖБ

Дроны-пожарные могут существенно повысить скорость реагирования и снизить риски для людей в ряде ситуаций, особенно в начале возгораний или в труднодоступных местах.

Скорость реагирования

Дрон может быть **запущен автоматически** или оператором сразу после получения уведомления о возгорании

У пожарных время реагирования **зависит от местоположения команды**, наличия транспорта и дорожных условий

Мониторинг после пожара

Дрон может **продолжать мониторинг** зоны после тушения, чтобы убедиться в отсутствии повторного возгорания

Для мониторинга могут требоваться **дополнительные ресурсы**, а нахождение людей в зоне пожара продолжительное время **небезопасно**

Автоматизация и автономность

Дрон может **работать автономно**, выполняя первичные задачи по тушению пожара без вмешательства оператора

В основном **требуют ручного управления** и участия человека, что делает их более зависимыми от человеческих факторов

Среднее время прибытия пожарных служб ~10 минут



Дрон отправляется к очагу возгорания **моментально**

ОБНАРУЖЕНИЕ ЛЕСНЫХ ПОЖАРОВ

Распределенная информационная система мониторинга лесных территорий на основе машинного зрения, искусственного интеллекта и беспилотных летательных аппаратов



Экспериментальные исследования направлены на повышение эффективности классических и нейросетевых алгоритмов детектирования и идентификации очагов возгорания, дыма в видимом и ИК диапазоне при съемке в различных погодных условиях и разное время суток

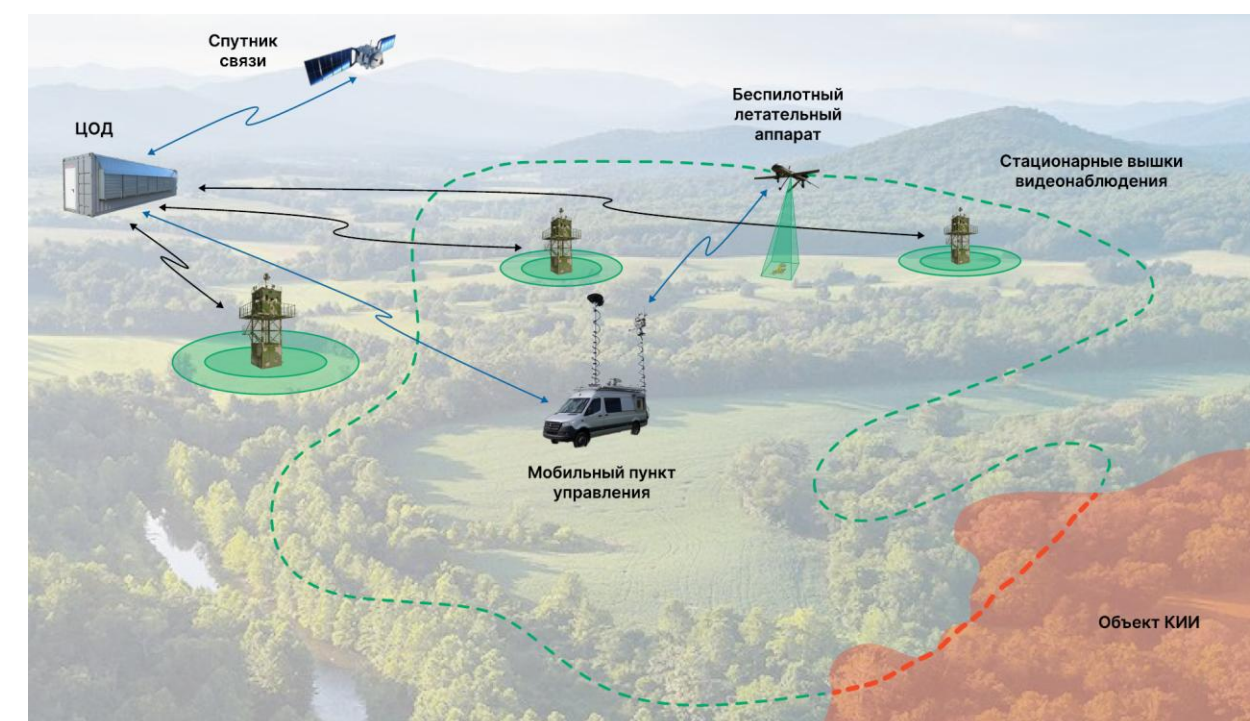


В результате НИР будут созданы:

- Экспериментальный образец (ЭО) специализированной мобильной лаборатории с применением БПЛА с длительным временем полета.
- ЭО мультиспектрального комплекса видеонаблюдения для стационарных и мобильных комплексов наблюдения.
- Конструкция и ЭО стационарного комплекса наблюдения.
- Аппаратно-программный комплекс мониторинга лесных массивов, включающий распределённую систему сбора, обработки и хранения данных, сеть связи объединяющую стационарные и мобильные комплексы наблюдения с мобильным пунктом управления и ЦОД.
- Система связи и передачи данных на больших территориях, на основе современной энергоэффективной ЭКБ.
- Программные средства превентивного обнаружения пожаров и других техногенных катастроф с применением машинного зрения и искусственного интеллекта.



Важной особенностью системы является **киберзащищенность системы управления**, это позволит безопасно применять БПЛА в непосредственной близости объектов КИИ



Типовые проблемные вопросы автономности БТС

1. Позиционирование себя в пространстве.
2. Необходимость доступа к картографии и привязка к сотовым сетям.
3. Несовершенство программного обеспечения и моделей ИИ.
4. Кибербезопасность.
5. Слабо предсказуемое поведение других участников движения.
6. Плохие погодные условия.
7. Радиоэлектронная защита и радиоэлектронная совместимость.

Максимальное время автономного движения БТС около **2 мин.**

СФЕРА ПРИМЕНЕНИЯ ЦИФРОВОЙ ПЛАТФОРМЫ БТС

Ключевые стейкхолдеры:

Министерство транспорта Российской Федерации



Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации



Разработчики беспилотных транспортных средств



Организации строящие и эксплуатирующие дороги



Объекты применения:

Автоматизированные системы контроля и управления движением БТС

Беспилотные транспортные средства

Системы сбора и обработки телеметрии дорожной инфраструктуры

Проработаны требования с Министерством транспорта Российской Федерации

СИСТЕМА УПРАВЛЕНИЯ ПРОЕКТАМИ СТРОИТЕЛЬСТВА АВТОМОБИЛЬНЫХ ДОРОГ

6

Система управления проектами строительства (сетей) автомобильных дорог – система управления жизненным циклом (сетей) автомобильных дорог которые обеспечат:

- формирование геологических моделей в рамках инженерных изысканий;
- контроль в ходе проектирования, строительства, эксплуатации, ремонта, реконструкции;
- управление технической документацией на этапах эскизного и технического проектирования, разработки рабочей конструкторской документации, строительства, эксплуатации, ремонта, реконструкции;
- планирование выезда на ремонт (реконструкцию) дорог с учетом общей пропускной способности сети дорог;
- гармонизацию планов реконструкции и строительства дорог федерального, регионального и муниципального значения.

Реализация проекта (ГОСТ Р 56294-2014):

- создание диспетчерского центра мониторинга и контроля строительства автомобильных дорог;
- внедрение BIM и цифровых двойников;
- Создание системы сбора данных о ходе строительства, состоянии дорожных объектов, сооружений;
- Визуализация текущего состояния транспортной системы;
- Реализация системы поддержки принятия решений;
- Внедрение организационно-распорядительного тракта для обеспечения функций управления с контролем исполнения задач (поручений);
- Сбор, обработка, хранение, верификация BIM-моделей, своевременное предоставление доступа подрядным организациям и сторонним сервисам.



ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ БЕСПИЛОТНЫХ И ПИЛОТИРУЕМЫХ ТРАНСПОРТНЫХ СРЕДСТВ

8

Организация информационного взаимодействия производится для:

- Повышения безопасности движения.
- Информирования водителей о дорожной обстановке.
- Безопасности совместного использования транспортной сети беспилотными и пилотируемыми транспортными средствами.
- Повышения пропускной способности транспортной сети.

Реализуемые формы взаимодействия между ТС:

- Электронные стоп-сигналы.
- Электронно-связанные автопоезда.
- Системы информирования о дорожном движении.

Реализуемые формы взаимодействия между ТС и внешней средой:

- Системы информирования аварийно-спасательных служб и участников движения.
- Дорожные сервисы.

Информационное взаимодействие обеспечивается за счет внедрения существующих стандартов и протоколов обмена данными и информацией (simTD, C-V2X, ГОСТ Р 57483, Bluetooth, IEEE 802.11p, LTE и др.) в рамках навигационного автомобильного комплекса.

Назначение и задачи элементов организации информационного взаимодействия:

- Электронные стоп-сигналы, позволяют реагировать на попомому транспортных средств, даже если они могут быть закрыты (например, другими транспортными средствами).
- Электронно-связанные автопоезда, позволяют транспортным средствам близко (до нескольких сантиметров) следовать за ведущим транспортным средством, получая по беспроводной сети информацию об ускорении и рулевом управлении.
- Системы информирования о дорожном движении, позволяют предоставлять самые свежие отчеты о препятствиях в систему навигации.
- Системы информирования аварийно-спасательных служб и участников движения, позволяют распространять информацию о ДТП и его последствиях используются для сокращения задержек и ускорения аварийно-спасательных операций для спасения жизни раненых.
- Дорожные сервисы, позволяют предоставлять информацию о товарах и услугах на дороге, обмениваться сообщениями, запросами и предложениями между участниками движения и дорожной инфраструктурой.



ЕДИНЫЙ ТРАНСПОРТНЫЙ ДОКУМЕНТ

5

Единый транспортный документ – средство (услуга), позволяющее оформить «единый билет» на весь маршрут поездки с использованием различных видов транспорта

Преимуществами мультимодальных пассажирских перевозок для пассажиров является:

- гарантированность перевозки по всему пути следования при планировании маршрута поездки разными видами транспорта;
- максимально удобная стыковка рейсами – сокращение времени, расстояния и количества пересадок;
- сохранение истории поездки;
- единая оплата всего маршрута и фиксированная стоимость поездки;
- простота и удобство оплаты при оформлении билета онлайн;
- обеспечение круглосуточного сопровождения пассажиров на маршруте;
- возможность управления проездными документами и маршрутами перемещения подконтрольных пассажиров (детей, родственников, командированных лиц);
- единый аккаунт парковок, каршеринга, такси, аренды велосипедов, самокатов и городского транспорта;
- управление льготами, оформление поездок в кредит.

Преимуществами мультимодальных пассажирских перевозок для ведомств и организаций является:

- борьба с нелегальными «серыми» перевозчиками;
- возможность контролировать перемещение пассажиров определенных социальных групп;
- возможность блокировать перемещение опасных пассажиров;
- ретроспективный анализ транспортного и пассажирского потоков;
- единая биллинговая система;
- единый личный кабинет пассажира;
- контроль деятельности агрегаторов и операторов транспортных услуг;
- интеграция со внешними БД и ИС;
- предоставление платных сервисов внешним потребителям на основе формирующегося банка данных.



РАЗРАБОТКА МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПИЛОТНОГО ТРАНСПОРТА

7

- Анализ факторов угроз информационной и кибербезопасности беспилотных транспортных средств.
- Разработка системы моделей угроз и нарушителей информационной и кибербезопасности беспилотных транспортных средств.
- Разработка общей и частных моделей по видам транспорта: автомобильный, железнодорожный, морской, речной, воздушный.
- Выработка мер (разработка рекомендаций) защиты от угроз информационной и кибербезопасности беспилотных транспортных средств.
- Разработка нормативно-методической документации в области информационной и кибербезопасности беспилотных транспортных средств.



СИСТЕМА СБОРА ДАННЫХ ТЕЛЕМЕТРИИ МОБИЛЬНЫХ (ПОДВИЖНЫХ) ОБЪЕКТОВ

9

- Мониторинг состояния транспортной сети с целью выявления вновь возникающих факторов снижающих безопасность транспортной сети.
- Сбор погодной информации с автотранспортных средств и других подвижных объектов, оснащенных CAN-шиной, с привязкой к координатам данного объекта.
- Построение карты реальной погоды в текущий момент времени и прогноза на час.
- Предупреждение гололеда, тумана, выпадения осадков и как следствие аварийности.
- Выработка рекомендаций по скоростному режиму на основе собранных данных и доведение через навигаторы и информационные табло водителям.



НАПРАВЛЕНИЯ РАБОТ

1

ДОПОЛНИТЕЛЬНЫЕ НАПРАВЛЕНИЯ РАБОТ

10

Интеграция информационных ресурсов Министерства транспорта Российской Федерации и подведомственных организаций

- Интеграция существующих (унаследованных) и вновь создаваемых автоматизированных информационных систем, комплексов средств автоматизации Министерства транспорта Российской Федерации и подведомственных организаций в рамках единого информационного пространства;
- Решение задач сбора, накопления, обработки, хранения данных от источников, доведения их до потребителей (специальных задач (СПО), пользователей);
- Разработка ведомственной программной интеграционной платформы на отечественных технологиях, которая предоставит возможность построения автоматизированных информационных систем класса 1Б;
- Безопасность объектов транспортной инфраструктуры: управление и контроль состояния всех инженерных систем и оборудования из единого центра; защита критически важных объектов инфраструктуры и систем управления движением.

Система прогнозирования и предупреждения ДТП

- Создание системы сбора данных о ДТП и анализа причин их возникновения;
- Разработка моделей поиска аналогичных мест (участков) на существующей транспортной сети;
- Выработка рекомендаций по повышению безопасности движения на выявленных аварийноопасных участках;
- Исключение (предупреждение) постройки аналогичных участков без принятия мер повышающих безопасность движения;
- Мониторинг состояния транспортной сети с целью выявления вновь возникающих факторов снижающих безопасность транспортной сети.

