

ЦИФРОВАЯ ПЛАТФОРМА ДЛЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ БЕСПИЛОТНОГО ТРАНСПОРТА

В.А. Минаев, А.С. Толпыгин

Цифровая трансформация транспортного комплекса России сопровождается активным внедрением новых технологий, созданием мультимодальных транспортных систем, применением беспилотных транспортных средств, управляемых искусственным интеллектом. Безопасность на транспорте неразрывно связана с кибербезопасностью систем управления. В статье рассматриваются решения, заложенные в ядро цифровой платформы, обеспечивающих защиту информации и киберустойчивость систем управления (СУ) беспилотных авиационных систем. Цифровая платформа беспилотных авиационных систем разрабатывается как инструмент и системотехническая основа для создания автоматизированных систем контроля и управления беспилотным транспортом, обеспечения их быстрого масштабирования за счет тиражирования унифицированных модулей. Подсистема защиты информации цифровой платформы создается в соответствии с требованиями регуляторов ФСТЭК России, Минобороны России и ФСБ России и в соответствии с требованиями к системе защиты информации, опирающейся на систему моделей угроз и нарушителей, рассмотренную в [1]. Особое внимание уделяется защите систем искусственного интеллекта, применяемым для управления беспилотными авиационными системами.

Ключевые слова: кибербезопасность, беспилотный транспорт, искусственный интеллект, модели угроз и нарушителя, цифровая платформа.

Введение

Стратегия развития беспилотной авиации Российской Федерации на период до 2030 г. и на перспективу до 2035 г. предусматривает:

– разработку скоростных транспортных беспилотных авиационных систем (БАС) для региональных, межрегиональных перевозок, в том числе – применительно к условиям Арктики;

– создание и развитие сетевой структуры разработки и производства беспилотных авиационных систем;

– создание системы идентификации и контроля БАС;

– формирование системы обеспечения комплексной безопасности применения БАС и их ключевых компонентов, включая системы искусственного интеллекта (ИИ);

– интеграцию БАС в единое воздушное пространство.

Для достижения поставленных целей требуется создать инфраструктуру, обеспечивающую полеты беспилотных воздушных судов (БВС), разработать стандарты и нормативные документы, заместить импортное оборудование и

программное обеспечение (ПО), зачастую не сопрягаемые друг с другом.

Возникает необходимость создания системы контроля и управления [1], основой которой будет отраслевая цифровая платформа БАС, обеспечивающая:

– быстрое создание и запуск типовых центров контроля и управления БВС;

– интеграцию БАС с информационно-управляющими системами (ИУС) пилотируемой авиации;

– создание федеральной системы контроля и управления движением БВС;

– интеграцию с системами учета БВС, планирования полета БВС, подачи планов полетов;

– создание маркетплейса, где все участники могут оформить свои отношения друг с другом: приобрести (взять в аренду) БВС, сдать (продать полетное время) БВС; застраховать БВС и ответственность перед третьими лицами; подать заявку по ОрВД (организации воздушного движения) и согласовать полет; узнать об ограничениях движения в воздушном пространстве;

- регистрацию и идентификацию БВС, расчет оптимального плана полета и согласование полетного задания;

- кибербезопасность БАС, защиту информации и персональных данных участников информационного взаимодействия;

- контроль исполнения полетного задания;

- моделирование поведения БВС и воздушной обстановки с применением цифровых двойников.

По прогнозам на основе данных из открытых источников, отчетов и исследований, опубликованных на сайте Национальной технологической инициативы (НТИ) [2], в 2026 году в воздушном пространстве будет постоянно находиться более 2 млн. БВС. Предельный же размер контролируемой группировки в настоящее время заявляется до 10 тыс. БВС.

Бесконтрольное применение БВС создает риски возникновения чрезвычайных ситуаций и совершения противоправных действий, включая проявления терроризма. Системное решение данного вопроса и предотвращения подобных инцидентов требует реализации в цифровой платформе функций, которые обеспечат:

- полный контроль трафика в границах зон защищаемых объектов, в том числе – критической инфраструктуры;

- киберустойчивость БВС и защиту их от неправомерного применения;

- контроль выполнения полетных заданий, выявление и предотвращение аномалий в поведении БВС;

- соответствие БВС законодательству РФ и требованиям регуляторов по безопасности их применения.

Таким образом, цифровая платформа становится центральным элементом, который обеспечит построение федеральной сети центров контроля и управления БАС на единых системотехнических принципах. Объединит указанные центры в общую информационно-аналитическую систему контроля и управления беспилотным транспортом. Обеспечит быстрое создание, запуск и масштабирование системы, интеграцию с существующими

интеллектуальными системами управления транспортом, построение единого пространства кибербезопасности.

Важность решения указанных задач возрастает в связи с появлением полностью автономных или управляемых БВС с минимальным участием оператора.

Киберустойчивость таких БАС в достаточной мере не изучена, чтобы гарантировать их безопасное применение в современных мегаполисах и защиту критически важных объектов.

В ходе авторских исследований, направленных на формирование требований к цифровой платформе и научно-технического задела для ее создания поставлены задачи проведения анализа:

- существующих и перспективных технических средств и информационных систем (ИС) контроля и управления движением БВС, перечня критически важных технологий, необходимых для создания цифровой платформы БАС;

- систем и средств организации защищенного информационно-технического взаимодействия (ИТВ) и обеспечения киберустойчивости БАС и инфраструктуры;

- систем ИИ для управления БВС и выявления аномалий в их поведении;

- нормативно-правовых актов (НПА) и нормативно-методической документации в области кибербезопасности БАС;

- факторов угроз кибербезопасности БАС;

- и создания модели угроз, а также нарушителей кибербезопасности БАС;

- и разработки мер по защите от угроз кибербезопасности БАС;

- и построения кроссплатформенного (в отношении аппаратных и операционных систем) ядра цифровой платформы БАС;

- и создания макета типового центра контроля и управления движением БВС;

- и разработки технического задания на опытно-конструкторскую работу по созданию сети центров контроля и управления движением БВС;

- и совершенствования НПА РФ в области кибербезопасности БАС.

Важнейшей задачей выступает также разработка моделей и методов

искусственного интеллекта для выявления аномалий в движении БВС; управления крупными скоплениями БВС в реальном времени; обнаружения и идентификации БВС с использованием нейронных сетей; управления воздушным движением БВС, подготовкой принятия решений, повышения уровня безопасности полетов БВС.

С учетом изложенного, определим триединую цель разработки цифровой платформы БАС:

- разработка инструментария для создания типовых центров контроля и управления движением БВС;
- построение распределенной защищенной информационно-аналитической системы контроля и управления движением БАС;
- интеграция системы контроля и управления БАС с системами управления пилотируемой авиации.

Для создания системы защиты информации цифровой платформы определены ее архитектура и функциональные подсистемы, уровень конфиденциальности обрабатываемой информации в них; интерфейсы взаимодействия.

Средства защиты информации предусмотрены на уровне интеграционной шины – ядра платформы.

Архитектура цифровой платформы строится вокруг интеграционной шины, которая обеспечивает объединение всего множества БВС, типовых пунктов контроля и управления БВС в единую интегрированную сетевую вычислительную среду (ИСВС), в рамках которой обеспечивается решение перечисленных задач (рис.1).

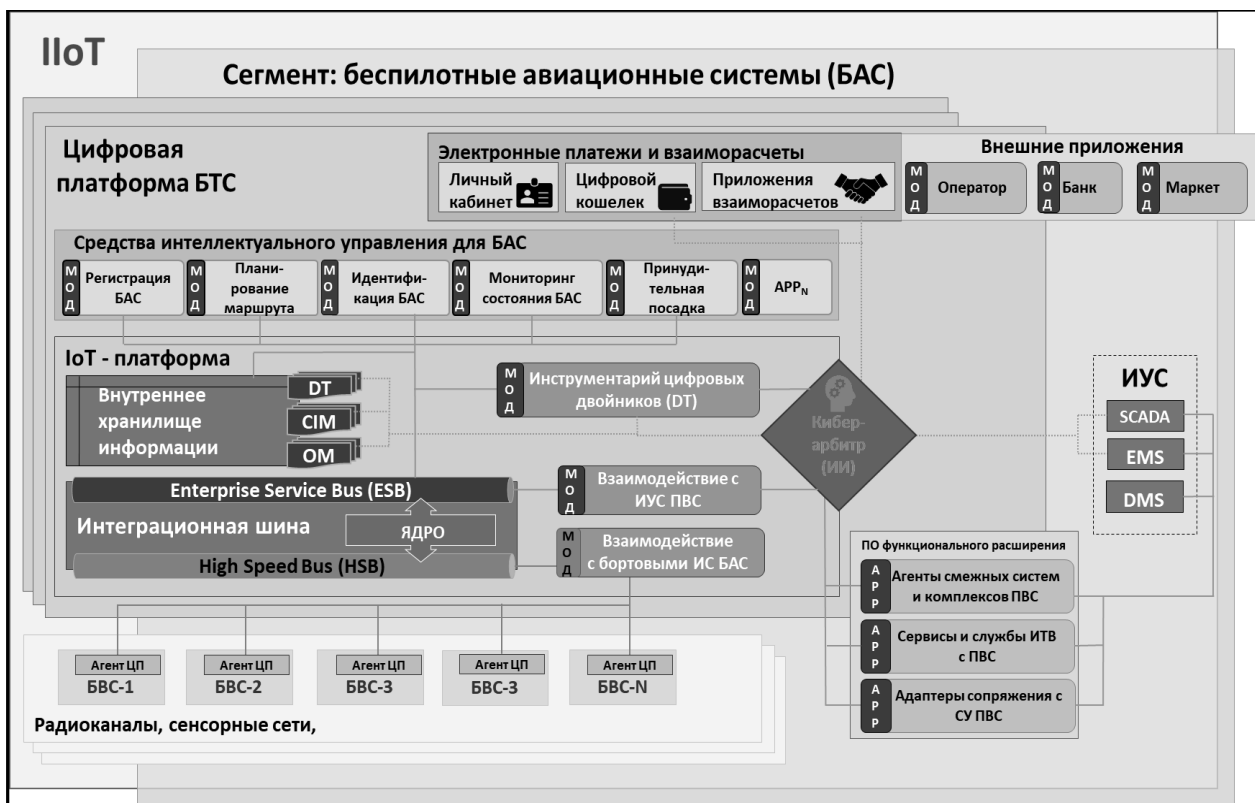


Рис. 1. Архитектура платформы БАС

Цифровая платформа состоит из:
 1) *Интеграционной* шины, обеспечивающей взаимодействие всех компонентов системы и решающей задачи:
 – создания единого адресного и информационного пространства на

множестве узлов гетерогенной вычислительной сети, состоящей из центров управления и бортовых комплексов беспилотных авиационных судов различных производителей;

- управления всеми процессами, зарегистрированными в соответствии с общесистемными требованиями;

- высокоскоростного обмена данными по сервисной шине (High Speed Bus) для взаимодействия с бортовыми системами БАС со скоростью обмена не менее 250 Кб/с;

- маршрутизации данных, гарантированного доведения информации, в том числе – по каналам с потерями и низкой пропускной способностью, гарантированной обработки информации получателем;

- гарантированного хранения данных во внутреннем хранилище и управления источниками данных, в том числе – внешними;

- разграничения доступа к информационным ресурсам;

- контроля действий всех субъектов (люди/роботы);

- бесшовной интеграции с внешними информационными системами и предоставления для них шины для обмена информацией с раскрытием семантики и общесистемных классификаторов.

2) Комплекса программ

интеллектуального управления БАС.

Комплекс включает модули мониторинга и интеллектуального управления, которые обеспечивают:

- начальную проверку, включение и контроль параметров работы модулей БАС;

- сбор, анализ и передачу результатов контроля модулей;

- управление электропитанием и параметрами работы модулей;

- обслуживание и управление конфигурацией модулей.

3) Интегрированного хранилища информации.

Хранилище включает банки данных первичной (собираемой) и вторичной (обработанной) информации. Обеспечивает хранение данных и предоставление доступа к ним, документам, моделям и алгоритмам обработки данных.

4) Модуля, реализующего инструментарий цифровых двойников.

Инструментарий цифровых двойников позволяет перенести в вычислительную среду сложившиеся представления (знания) о состоянии всей системы управления и объективизировать их на уровне концептуальной модели предметной области (КМПО), обладающей, в том числе и темпоральными свойствами [3].

5) Модуля искусственного интеллекта (киберарбитр) [4].

Модуль реализует алгоритмы интеллектуальных вычислений с применением нейронных сетей для обработки сигналов, больших данных, разрешения конфликтов субъектов информационного взаимодействия. На БВС предусмотрены модели машинного зрения.

В условиях быстро изменяющейся воздушной обстановки и переменного состава группировки в воздухе обеспечивается динамическое распределение вычислительных ресурсов флота БЛА, повышается энергоэффективность.

6) Модуля взаимодействия с бортовыми информационными системами БАС предыдущих поколений и сторонних разработчиков [5].

Модуль позволяет решать проблемы интеграции разнородных БЛА и БАС и обеспечить их взаимодействие на основе унифицированных протоколов.

7) Модуля взаимодействия с информационно-управляющими системами пилотируемых воздушных судов.

Модуль обеспечивает интеграцию БАС в единое информационное пространство воздушного движения.

Исходя из сказанного, укажем принципы, положенные в архитектуру цифровой платформы, и которые позволяют:

- производить реконфигурацию системы и ее составных частей без изменения архитектуры;

- унифицировать и типизировать модули технического конструктива, а также библиотеки базовых алгоритмов;

- гибко изменять состав встроенного и системного ПО;
- работать с любыми операционными системами (ОС) реального времени (RV) и обеспечивать кроссплатформенность;
- резервировать аппаратные и программные компоненты и обеспечивать требуемую кибербезопасность, надежность, отказоустойчивость БАС.

Предполагается функционирование ПО цифровой платформы на отечественных аппаратных средствах Эльбрус.

Используемые подходы и методы позволят создать класс технологий для построения унифицированной ИСВС, которая

в дальнейшем будет взаимодействовать со всеми используемыми и перспективными беспилотными авиационными системами.

Ядро цифровой платформы и встроенные средства защиты информации

Ключевой элемент цифровой платформы БАС – интеграционная шина, предназначенная для организации вычислительного процесса на множестве распределенных в пространстве гетерогенных программно-аппаратных средств БАС.

Рассмотрим подробнее ее устройство. На рис. 2 представлена структурно-функциональная схема интеграционной шины.

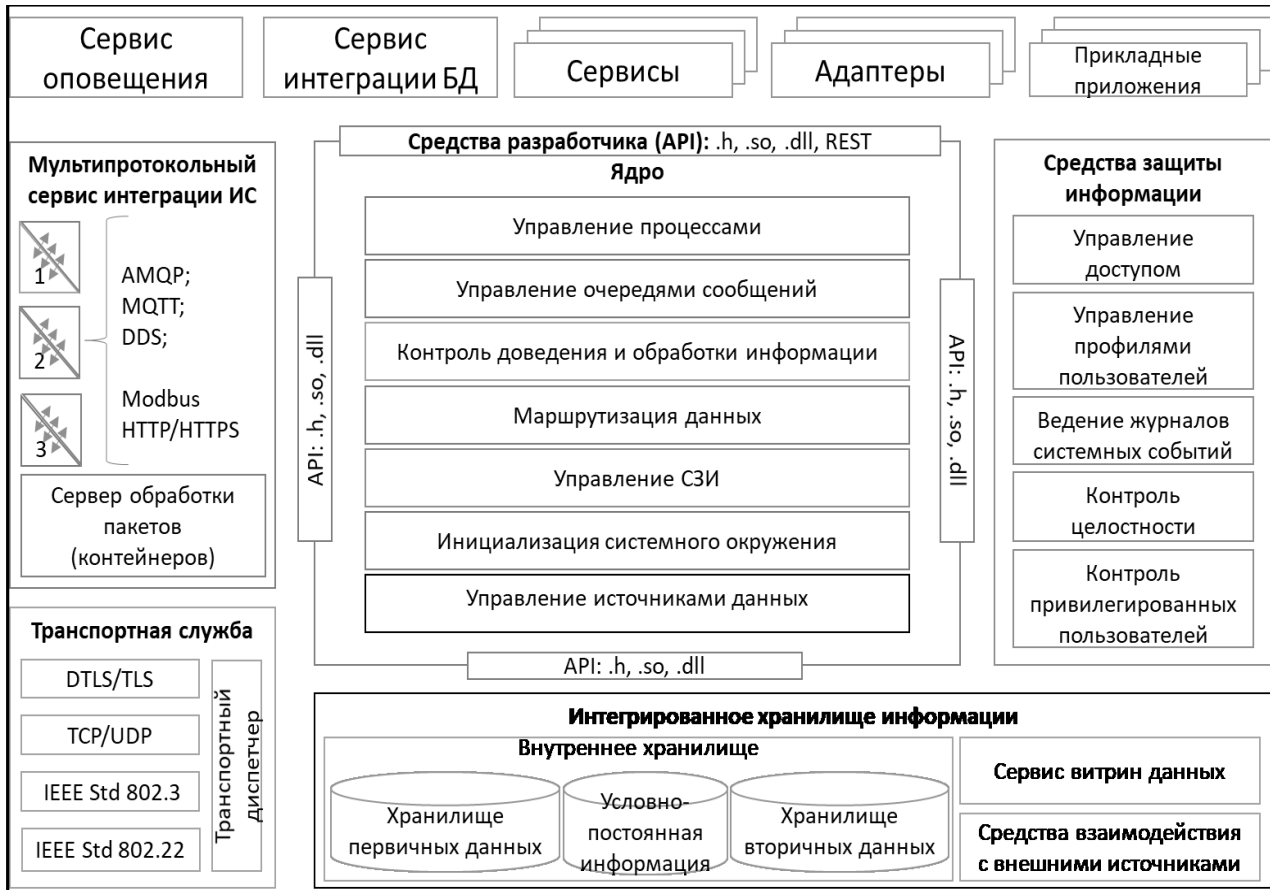


Рис. 2. Структурно-функциональная схема интеграционной шины – ядра цифровой платформы БТС

В составе интеграционной шины – пять функциональных подсистем:

- организации и управления вычислительным процессом – ядро интеграционной шины;
- интегрированное хранилище информации;
- комплекс средств защиты информации;

- транспортная служба передачи данных;
- мультипротокольный сервис интеграции информационных систем.

Модуль инициализации системного окружения, находящийся в составе ядра, обеспечивает единое адресное пространство на всем множестве узлов (вычислительных установок, логических модулей) и задач, а

также единую среду функционирования для всех приложений, зарегистрированных и выполняющих общесистемные соглашения. К приложениям относятся также сервисы, адаптеры сопряжения и различное программное обеспечение, решающее прикладные задачи. При инициализации системного окружения логический модуль получает системные переменные, справочники и классификаторы информации, адресные таблицы, правила обработки документов и сообщений, данные об организации вычислительного процесса на объекте автоматизации, матрицу разграничения доступа к информационным ресурсам и каналам передачи данных.

Модуль управления очередями сообщений интеграционной шины для каждого зарегистрированного процесса обеспечивает ведение очереди сообщений с возможностью установки приоритетов их обработки.

Штатная функция ядра – маршрутизация данных, выполняется модулем маршрутизации в зависимости от вида и формата данных передаваемых сообщений и документов.

В функциональные возможности шины заложена возможность работы на низкоскоростных каналах (до 1200 бод) с потерями. Интеграционная шина контролирует целостность передаваемых данных, контролируется доведение и обработка данных специальным обработчиком на приемной стороне.

Модуль управления средствами защиты информации обеспечивает управление встроенным комплексом средств защиты информации (КСЗИ) интеграционной шины, включающим средства:

- управления доступом;
- управления профилями пользователей;
- ведения журналов регистрации системных событий;
- контроля целостности;
- контроля действий привилегированных пользователей.

В функции модуля управления доступом входит контроль выполнения всех операций доступа к информационным ресурсам и каналам связи производимых субъектами

доступа средствами цифровой платформы БАС.

Модуль управления профилями пользователей обеспечивает управление полномочиями субъектов. Поддерживаются мандатная, дискреционная и ролевая модели управления доступом.

Все инциденты нарушения информационной безопасности и штатного режима функционирования фиксируются в журнале регистрации системных событий КСЗИ.

Развитие системы защиты информации видится в обеспечении кибербезопасности платформы с функциями искусственного интеллекта, защиты ее от угроз, приводящих к:

- ошибкам в моделях обработки данных;
- несанкционированному получению конфиденциальной информации путем обмана модели искусственного интеллекта;
- преднамеренному внесению некорректных данных с целью манипуляции искусственным интеллектом и искажения результата работы системы ИИ;
- переусложнению системы ИИ.

Взаимодействие БАС и цифровой платформы реализуется посредством многопротокольного сервиса интеграции, а также разрабатываемых по мере необходимости адаптеров сопряжения.

Инструментарий цифровой платформы БАС позволяет разработчикам ПО для БАС реализовывать любые дополнительные интеграционные механизмы обеспечения ИТВ с внешними информационно-управляющими системами БАС. Обязательными условиями являются выполнение общесистемных соглашений. Это позволяет включать новые элементы и ресурсы в единое информационное пространство. Обеспечивать централизованное управление ими, предоставлять доступ к данным и обеспечивать защиту информации.

Технологическая зрелость цифровой платформы

Программное обеспечение, в составе цифровой платформы, характеризуется следующими свойствами:

– исходные коды являются оригинальными и не имеют заимствований из Интернета и других открытых источников;

– программное обеспечение авторизовано – за каждой строчкой кода есть ответственный автор – резидент РФ;

– высокая степень готовности ядра цифровой платформы и ее компонент;

– разработка ориентирована на сертификацию по требованиям МО, ФСБ, ФСТЭК РФ;

– технологический цикл выстраивается в соответствии с требованиями, предъявляемыми в [6].

Уровень зрелости технологий и продуктов в составе цифровой платформы представлен в табл. 1. В поле «статус» указан

условный уровень зрелости технологии, продукта:

PRO – промышленное исполнение продукта (изделия), имеются внедрения и накоплен опыт применения в реальных условиях.

MVP (Minimum Viable Product) – минимально жизнеспособный продукт, для которого подтверждена бизнес-ценность посредством проверки гипотез.

ADV TECH – уровень зрелости, при котором разработан и протестирован в реальных условиях экспериментальный образец или работающий прототип изделия.

TECH – технология или продукт протестированы на макетах в рамках инициативных НИР.

Таблица 1

Уровень зрелости технологий и продуктов в составе цифровой платформы

Технологии, продукты	Статус
Интеграционная шина <ul style="list-style-type: none"> ▪ 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 ▪ Комплекс средств защиты информации 	PRO
Система операционного управления <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> ▪ Очередь заданий на перемещение БТС ▪ Монитор состояний транспортной сети ▪ Построение карты погоды ▪ Выработка рекомендаций скоростного режима ▪ Расчет мультимодальных поездов 	TECH
Интегрированное хранилище информации и объединенный коммуникационный центр консолидации данных от разнородных источников БАС	ADV TECH
Агентство доступа к первичным сетям передачи данных	ADV TECH
Интерактивный экспресс-анализ данных <ul style="list-style-type: none"> • Служба экспресс-анализа серий данных 	TECH

Уровни зрелости, примененные для оценки составных элементов цифровой платформы, можно условно отождествить с уровнями готовности технологий (УГТ), определенными ГОСТ Р 58048-2017. В табл. 2 представлено соотнесение с

условными ограничениями, обусловленными особенностями технологического цикла разработки ПО цифровой платформы и наличием доступных действующих аналогов.

Соответствие уровня зрелости технологий и продуктов УГТ по ГОСТ Р 58048

УГТ по ГОСТ Р 58048-2017		Уровень зрелости элементов ЦП БАС
УГТ	Описание	
УГТ-4	Компонент и/или макет испытан в лабораторных условиях	TECH
УГТ-6	Модель системы/подсистемы или прототип продемонстрирована в условиях, близких к реальным	MVP*
УГТ-7	Прототип системы продемонстрирован в реальных условиях эксплуатации	ADV TECH
УГТ-9	Работоспособность системы подтверждена в ходе успешной эксплуатации (достижения цели)	PRO

Примечание. * – MVP не соответствует УГТ-3, как это предполагает изначальный замысел и назначение MVP, а соответствует УГТ-6, ввиду того, что для технологий и продуктов в составе платформы, возможность демонстрации открывается после создания прототип.

Заключение

Развитие беспилотного транспорта – приоритетное направление обеспечения технологического суверенитета РФ, важным элементом которого является применение отечественной научной, технической и технологической базы.

Разработка рассмотренной в статье цифровой платформы ведется без заимствования зарубежных технологий, в том числе из открытых источников. Отдельные компоненты платформы проходили сертификацию по требованиям безопасности информации в системах сертификации ФСТЭК России, Минобороны России, ФСБ России в составе систем и изделий, эксплуатируемых в государственных организациях

Технологии реализуемые на уровне ядра цифровой платформы, позволяют снять ряд ограничений при построении информационно-управляющих систем БАС, а именно:

- использование различных опорных сетей связи и передачи данных;
- работа в низкоскоростных, неустойчивых каналах связи;
- возможность взаимодействия с системами управления других видов беспилотного транспорта: автомобильного, морского, речного, а также роботами;
- организация мультимодальных перевозок;
- киберустойчивости БАС.

Выбранная архитектура цифровой платформы позволяет:

- создавать автоматизированные защищенные распределенные системы контроля и управления беспилотными авиационными системами на федеральном и региональных (ведомственных) уровнях;
- ускоренно создавать и вводить в действие типовые центры контроля и управления БАС и интегрировать их в единую автоматизированную систему;
- интегрировать в единую систему контроля и управления разнородные БАС различных разработчиков.

В рамках Федерального проекта «Развитие инфраструктуры, обеспечение безопасности и формирование специализированной системы сертификации беспилотных авиационных систем» платформа позволяет:

- создать унифицированную инфраструктуру обеспечения полетов БВС и своевременно оснастить ей субъекты РФ в соответствии с планом до 2030 г.;
- обеспечить контроль воздушной обстановки над защищаемыми объектами, включая критическую инфраструктуру;
- достичь требуемой киберустойчивости БАС и их защиту от неправомерного применения;
- контролировать выполнение полетных заданий, выявлять и предотвращать аномалии в поведении БАС;

– обеспечить соответствие БАС законодательству РФ и требованиям по безопасности.

Список литературы

1. Минаев В.А., Толпыгин А.С. Кибербезопасность и киберустойчивость беспилотных транспортных систем // Информация и безопасность. 2024. Т. 27. Вып. 2. С.177-184.

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

2. Национальная технологическая инициатива. URL: <https://nti2035.ru/markets/aeronet> (дата обращения: 23.08.2024).

3. Минаев В.А., Мазин А.В., Здирук К.Б., Куликов Л.С. Синтез цифровых двойников с применением многоаспектной рекурсивной декомпозиции // Вопросы радиоэлектроники. 2019. № 11. С. 26-37.

4. Гречанюк Ф.А., Здирук К.Б., Толпыгин А.С. Киберконтракт как

инструмент регулирования гражданско-правовых отношений в цифровой экономике / Тезисы доклада на XVI Всероссийской научной конференции. «Нейрокомпьютеры и их применение». Москва, 13 марта 2018 года. М.: Изд-во МГППУ, 2018. С. 376-377.

5. Здирук К.Б. Реализация задач сбора, консолидированной обработки и управления разнородными источниками данных процесса подготовки космонавтов при интеграции ФГБУ «НИИ ЦПК имени Ю.А. Гагарина» в единое информационное пространство ракетно-космической отрасли / Материалы XI Международной научно-практ. конференции «Пилотируемые полеты в космос». Звездный городок, Московской обл. 10-12 ноября 2015 года. Звездный городок: Научно-исследовательский испытательный центр подготовки космонавтов имени Ю.А. Гагарина, 2015. С. 119-121.

6. Проект национального стандарта ГОСТ Р 56939. Защита информации. Разработка безопасного программного обеспечения. Общие требования. URL: <https://fstec.ru/tk-362/standarty/proekty/proekt-natsionalnogo-standarta-gost-r-56939> (дата обращения: 23.08.2024).

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia
Московский государственный технический университет имени Н. Э. Баумана
Bauman Moscow State Technical University

Поступила в редакцию 15.08.24

Информация об авторах

Минаев Владимир Александрович – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: mlva@yandex.ru

Толпыгин Алексей Сергеевич – канд. техн. наук, доцент кафедры информационной безопасности Московского государственного технического университета имени Н. Э. Баумана, e-mail: tas59417@yandex.ru

**DIGITAL PLATFORM
FOR SECURE INFORMATION CONTROL SYSTEMS
OF UNMANNED VEHICLES**

V.A. MINAEV, A.S. TOLPYGIN

The digital transformation of the Russian transport complex is accompanied by the active introduction of new technologies, the creation of multimodal transport systems, and the use of unmanned vehicles controlled by artificial intelligence (AI). Transport security is inextricably linked to the cybersecurity of control systems (CS). The article discusses the solutions embedded in the core of the digital platform that ensure information protection and cyber stability of CS of unmanned aircraft systems (UAS). The digital platform is being developed as a tool and a system-technical basis for creating automated control and management systems for unmanned vehicles, ensuring their rapid scaling through the replication of unified modules. The information protection subsystem of the digital platform is created in accordance with the requirements of the regulators of the FSTEC of Russia, the Ministry of Defense of Russia and the FSS of Russia and in accordance with the requirements for an information protection system based on a system of threat and intruder models discussed in [1]. Special attention is paid to the protection of artificial intelligence systems used to control UAS.

Keywords: cybersecurity, unmanned vehicles, artificial intelligence, threat and intruder models, digital platform.

Submitted 15.08.24

Information about the authors

Vladimir A. Minaev – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V. Ya. Kikot Moscow University of the Internal Affairs Ministry, Moscow, e-mail: m1va@yandex.ru

Alexey S. Tolpygin – Cand. Sc. (Technical), Associate professor of the Information Security Department of Bauman Moscow State Technical University, Moscow, e-mail: tas59417@yandex.ru