DOI 10.36622/1682-7813.2024.27.2.003
УДК 004.896:004.56:007.52:008.2

КИБЕРБЕЗОПАСНОСТЬ И КИБЕРУСТОЙЧИВОСТЬ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СИСТЕМ

В.А. Минаев, А.С. Толпыгин

В статье рассматриваются вопросы обеспечения кибербезопасности беспилотного транспорта (БТ), характеризуются российские особенности его развития, анализируются угрозы кибербезопасности системам управления (СУ) БТ, предлагается подход к формированию актуальных угроз на этапах жизненного цикла СУ БТ – от формирования исходных требований до вывода систем из эксплуатации, рассмотрены иерархическая структура системы контроля и управления беспилотным транспортом и направления разработки системы моделей угроз кибербезопасности для беспилотного транспорта – базовой, частных и типовых, приводится алгоритм формирования множества угроз кибербезопасности СУ БТС, описываются угрозы системе управления в зависимости от уровня автономности транспортного средства. Особое внимание уделяется применению технологий искусственного интеллекта в СУ БТС. Делается вывод, что основной задачей киберзащиты является сохранение управляемости системой, требующей системного подхода к защите информации и инфраструктуры беспилотного транспорта от киберугроз. Кроме того, существует необходимость полного контроля трафика БТС в границах зон защищаемых объектов критической инфраструктуры, защиты от неправомерного применения БТС, контроля выполнения маршрутных (полетных) заданий, выявления и предотвращения аномалий в поведении БТС, соответствия законодательству России и требованиям регуляторов по безопасности их применения. Для этого необходимо создание сети центров контроля и управления движением БТС, обеспечивающих ситуационную осведомленность и поддержку управленческих решений.

Ключевые слова: кибербезопасность, киберустойчивость, беспилотный транспорт, искусственный интеллект, модель угроз, безопасность информации.

Введение

Беспилотный транспорт проникает во многие сферы нашей жизни и отрасли хозяйствования. Активно начали развиваться все его виды: автомобильный, авиационный, железнодорожный, морской. Беспилотные автомобили становятся неотъемлемой частью умных городов, строятся специализированные трассы с необходимой инфраструктурой для движения беспилотных автомобилей.

Разработкой беспилотных автомобилей занимаются не только крупнейшие автоконцерны, такие как Tesla, Ford, General Motors, BMW, Audi, Mercedes-Benz, Toyota, Nissan, Honda, Группа ГАЗ, Камаз, НАМИ, Меркатор Холдинг, но и многие развитые технологические компании – Сберавтотех, Яндекс, Apple, Baidu, Google, Nvidia, Uber.

В Москве и Республике Татарстан с 2018 г. ведется эксперимент по опытной эксплуатации беспилотных автомобилей на дорогах общего пользования [1].

Правовой режим эксперимента установлен постановлением Правительства РФ от 9.03.2022 № 309 [2].

С середины 2023 г. открыто движение беспилотных автомобилей по трассе М-11.

Беспилотные летательные аппараты (БПЛА) активно применяются для решения задач мониторинга объектов критически важной инфраструктуры городов (трубопроводы, линии электропередач, дорожная инфраструктура, система связи, вокзалы, аэропорты и др.); грузоперевозок в труднодоступные регионы и отдаленные территории; разведки в труднодоступных местах (геологоразведки, водного кадастра, мониторинга водных объектов).

Ряд стран, в их числе Германия, Россия, Япония проводят испытания беспилотных поездов. Норвегия, США, Турция и другие страны применяют беспилотные морские суда гражданского и специального назначения.

1. Российские реалии

По оценкам из открытых источников к 2027 году производство БПЛА в России достигнет 2 млн. шт. в год, на дорогах появится не менее 100 тыс. беспилотных автомобилей.

Однако в описанной благоприятной картине есть и негативная сторона. А именно, из-за подчас бесконтрольного применения беспилотных транспортных средств (БТС) расширяется возможность совершения противоправных актов: террористических, шпионских действий и других криминальных эксцессов.

Этому способствуют складывающаяся геополитическая обстановка, развитие высоко технологичных средств, тотальная цифровизация общественной жизни, имеющая и криминальные аспекты.

И хотя в России принимаются меры государственной поддержки, которые направлены на стимулирование развития беспилотного автомобильного транспорта и беспилотных авиационных систем (БАС), при этом наблюдается недостаток, а иногда – отсутствие необходимого регулирования в сфере беспилотного транспорта.

Для предотвращения указанных криминальных инцидентов необходима система, которая обеспечит:

– полный контроль трафика в границах важных социальных зон, 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 функционирования БТС законодательству РФ и требованиям регуляторов по безопасности их применения.

Отметим, что в сфере, относящейся к кибербезопасности, в последние годы появилось немало научных публикаций [3-7] и нормативных работ [8; 9].

Однако применительно к беспилотному транспорту эта проблема только начинает решаться учеными и специалистами, все более актуализируясь. Именно это и обусловило появление настоящей статьи. Оперируя понятиями «кибербезопасность», «киберустойчивость», авторы делают в ней акцент на том, что при защите систем управления БТС необходимо уделять особое внимание, в первую очередь, таким аспектам, которые связаны с действиями, направленными на нарушения в управлении движением, приводящими к авариям, крушениям, катастрофам и гибели пассажиров и иных членов общества.

Противоправные действия, связанные с кражей грузов, персональных данных или другой конфиденциальной информации, рассматриваются во вторую очередь.

2. Угрозы кибербезопасности

Под *угрозами кибербезопасности беспилотного транспорта* будем понимать *совокупность условий и факторов, создающих реальную или потенциальную опасность потери управления транспортной системой из-за нарушения конфиденциальности целостности, доступности информации, циркулирующей в системе управления БТС.*

Реализация угроз кибербезопасности, в первую очередь, связана с уязвимостями в системе управления БТС, которая представляет собой комплекс программно-аппаратных средств и каналов связи, обеспечивающих управление без участия человека.

Существующие системы управления беспилотным транспортом используют различные технологии, включая системы глобального позиционирования (ГЛОНАСС, GPS), радары, лидары, камеры, датчики и сенсоры, которые собирают информацию об окружающей среде. Программное обеспечение систем управления реализует алгоритмы и модели, которые обрабатывают эту информацию и принимают решения о движении БТС.

Важную роль в системах управления беспилотным транспортом играют технологии искусственного интеллекта. Он используется для обработки информации, принятия решений и управления БТС. Искусственный интеллект может использоваться для обучения моделей и алгоритмов, которые помогают БТС принимать решения о движении и обеспечивать безопасность. Он также может использоваться для анализа данных и

прогнозирования поведения участников дорожного движения.

Вместе с тем, необходимо учитывать киберугрозы инфраструктуре, необходимой для систем управления беспилотным транспортом. Она включает такие элементы как система связи, системы хранения и обработки данных, системы организации и управления движением, которые помогают БТС ориентироваться в пространстве и корректно двигаться по маршруту. Эти элементы могут быть как физическими, так и виртуальными.

Перечисленные элементы составляют объекты защиты системы управления БТС.

В качестве алгоритма формирования актуальных угроз безопасности информации систем управления БТС предлагается использовать подход, представленный на рис. 1.

Для оптимизации усилий при формировании перечня актуальных угроз безопасности информации предлагается первичный перечень угроз на начальном этапе ориентировать на Банк данных угроз (БдУ) ФСТЭК России (ubi.fstec.ru).

Типовые угрозы для системы управления БТС определенные для каждого этапа ее жизненного цикла, будут составить основу базовой модели угроз (БМУ).

Путем просеивания (исключения) из БдУ сформированы более 30 угроз, которые могут осуществляться с высокой вероятностью и иметь значительный уровень влияния.

Полный перечень угроз формируется добавлением киберугроз специфичных для систем управления БТС, которые выявляются при анализе факторов угроз, характерных конкретным типам БТС.

После обобщения выделены следующие группы угроз кибербезопасности беспилотного транспорта:

1. Угрозы безопасности данных, включающие:

– несанкционированный доступ к данным систем управления беспилотным транспортом;

– подмена данных, на основе которых принимаются решения по управлению движением БТС, например, маршрутное задание, данные об окружающей среде;

– кража личных (персональных) данных пассажиров и (или) конфиденциальной информации о маршруте их передвижения;

– внедрение вредоносных программ, которые могут влиять на системы управления и приводить к сбоям или утечке информации.

2. Угрозы безопасности связи, включают:

– подделку сигналов связи между БТС и системой управления;

– внедрение вредоносных программ, нарушающих работу систем связи с целью перехвата управления БТС.

3. Угрозы безопасности системам управления включают:

– ошибки в программном обеспечении, которые могут привести к сбоям или уязвимостям в системах управления;

– ошибки идентификации БТС и взаимодействующих элементов;

– уязвимости в аппаратном обеспечении, потенциально допускающие получение несанкционированного доступа к системам управления БТС.

4. Инфраструктурные угрозы безопасности характеризуются недостатками в системах:

– организации и управления движением, которые могут приводить к сбоям или уязвимостям в системах управления флотом БТС;

– связи, реализующиеся в их потере между БТС и внешней СУ.

Рис. 1. Алгоритм формирования множества угроз кибербезопасности СУ БТС

5. Угрозы безопасности системам искусственного интеллекта, такие как:

– внесение некорректных данных с целью манипуляции системой ИИ, преднамеренного искажения результатов работы и нарушения функционирования СУ БТС;

– ошибки (различной природы) в моделях обработки данных;

– получение конфиденциальной информации путем обмана системы ИИ;

– закладки в моделях с целью получения несанкционированного доступа к конфиденциальной информации, воздействия на результаты работы системы ИИ.

Следует отметить, что из-за незаконной санкционной политики Запада в отношении нашей страны затруднен доступ к международным базам уязвимостей и индикаторам компрометации, источникам данных об угрозах. Это частично приводит к «ослеплению» средств киберзащиты.

На это накладываются факторы продолжающейся эксплуатации зарубежного программного обеспечения (ПО) и ресурсов сети Интернет, а также отказов в технической поддержке IT-оборудования и обновления ПО со стороны недружественных государств. Очевидно, в этих условиях возрастает вероятность реализации кибератак на системы управления транспортом, а ее обеспечение необходимой защитой становится иногда нетривиальной задачей.

Поскольку уязвимости в СУ БТС могут быть внесены до начала эксплуатации, ее защиту необходимо обеспечить на всех этапах жизненного цикла: формирование требований; проектирование; разработка; ввод в действие; эксплуатация; вывод из эксплуатации.

С целью учета и систематизации всех возможных факторов угроз безопасности системам управления БТС и сфер проявления угроз необходимо разрабатывать модели угроз для каждого конкретного вида и класса БТС. С переходом на новые уровни автономности (УА) транспортных средств появляются новые уязвимости и новые угрозы системе управления, представлены в табл. 1.

Таблица 1

Угрозы кибербезопасности системе управления
в зависимости от уровня автономности (УА) транспортного средства

УА БТС	Характеристика уровня автономности	Угрозы СУ
УА-5	Полная автономность БТС. Пилот не требуется	Угрозы уровня 4 Угрозы, связанные с потерей контроля над системами искусственного интеллекта
УА-4	Полные возможности самостоятельного вождения. Пилот контролирует и управляет удаленно по радиоканалам	Угрозы уровня 3 Угрозы, связанные с перехватом управления. Угрозы искажения данных, от ошибок в данных, закладки в моделях ИИ.
УА-3	Ограниченные возможности самостоятельного вождения, БТС контролируется и при необходимости управляется пилотом	Угрозы уровня 2 Угрозы, связанные с возможным влиянием на корректность работы бортовых систем по каналам связи
УА-2	Частичная автоматизация и помощь водителю. Транспортным средством управляет компьютер.	Угрозы уровня 1 Угрозы, связанные с работой бортового компьютера, ошибками ПО, уязвимостями аппаратных средств
УА-1	Ассистенты пилота помогают в сложных условиях движения, при этом пилот контролирует всё (не предусмотрено автоматизированных систем вождения)	Угрозы уровня 0 Угрозы, связанные с некорректной работой ассистентов пилота
УА-0	Функций автоматизации и помощников нет. Транспортное средство полностью контролируется и управляется пилотом.	Угрозы, связанные с работой внешних систем организации и управления движением: светофоры, информационные табло

3. Система моделей угроз кибербезопасности

Для учета всех возможных факторов и проявлений угроз безопасности системам управления БТС необходимо разработать и поддерживать в актуальном состоянии модели угроз кибербезопасности для каждого вида и класса БТС, с учетом уровня автономности БТС. Подчеркнем, как и Марков А.С. [5], что «информационная безопасность» выступает более широким понятием по отношению к понятию «кибербезопасность», отражающего воздействия компьютерных атак.

Для обеспечения системности и единства подходов к решению вопросов кибербезопасности беспилотного транспорта предлагается разработать систему моделей угроз (МУ) информационной безопасности, адаптированных к конкретным видам, типам и уровням автономности БТС.

Предлагаемая система моделей угроз безопасности включает в себя три вида моделей:

– базовую МУ безопасности информации беспилотного транспорта, основанную на иерархии уровней автономности БТС;

– типовые МУ безопасности составных частей системы управления БТС;

– частные (по видам БТС) модели угроз (ЧМУ).

Структурная схема системы МУ безопасности для БАС приведена на рисунке 2. Типы БАС: С – самолетный, В – вертолетный, М – мультироторный, К – конвертоплан, Г – гибридный. Классы БАС:

СЛ – сверхлегкий (до 4 кг); Л – легкий (4-30 кг); С – средний (30-500 кг); Т – тяжелый (свыше 500 кг).

БМУ предназначена для управления информационной безопасностью на стратегическом уровне – уровне федерального органа исполнительной власти, ответственного за безопасность беспилотного транспорта в Российской Федерации.

БМУ является методическим документом для разработчиков БТС и разработчиков средств защиты информации для БТС, а также организаций, выполняющих работы по проектированию систем контроля и управления беспилотным транспортом, организаций, осуществляющих работы по оценке соответствия беспилотного транспорта требованиям защиты информации и его сертификации по требованиям регуляторов.

БМУ содержит описание объекта защиты в части структуры и функциональных характеристик СУ БТС, соответствующих им угроз безопасности информации и модели нарушителя, а также методические рекомендации по разработке типовых и частных МУ.

Базовая модель охватывает все стадии жизненного цикла БТС, в том числе – определяющие порядок разработки (проектирование, изготовление опытного образца и испытания), производства, эксплуатации и утилизации, определяет порядок и условия разработки: типовых моделей угроз безопасности центров контроля и управления движением для типовых элементов в СУ БТС; частных (по видам БТС) моделей угроз объектов (элементов) СУ БТС.

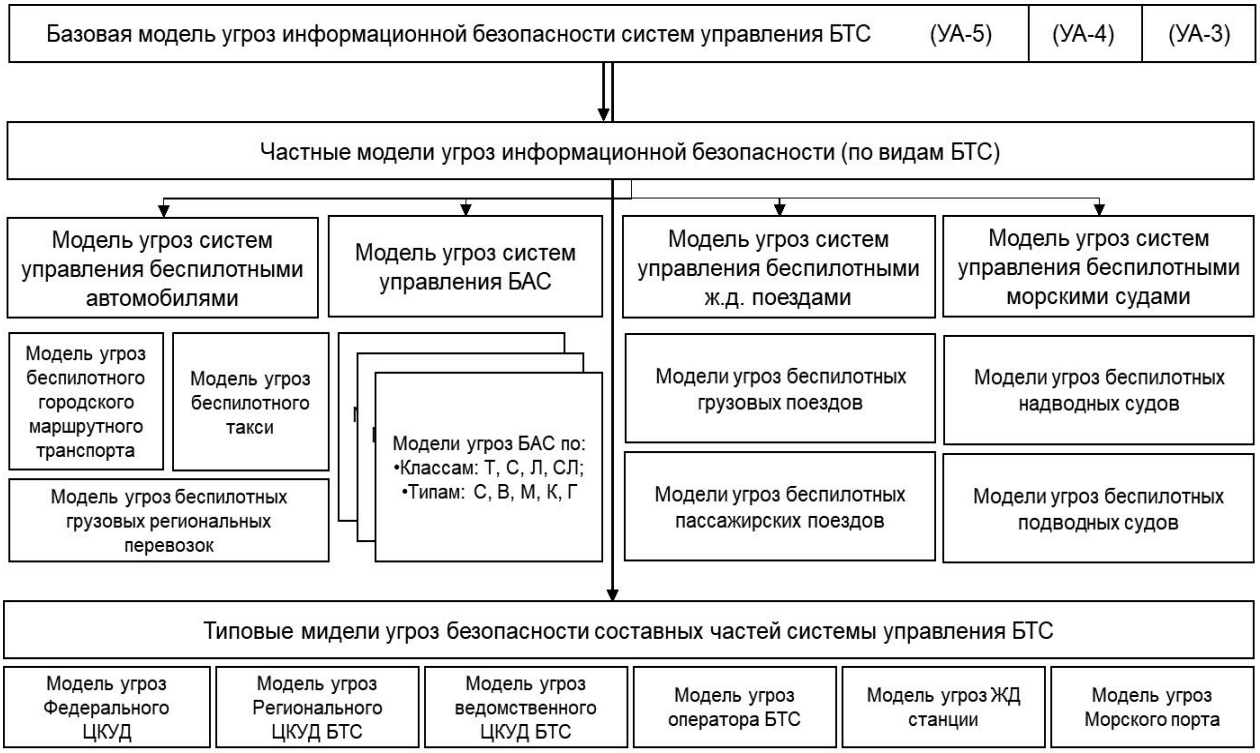

Рис. 2. Систематизация моделей угроз кибербезопасности беспилотного транспорта

Для поддержания моделей угроз всех видов в актуальном состоянии необходимо проводить их регулярное уточнение: при выявлении новых угроз, появлении новых способов и средств их реализации; при модернизации системы контроля и управления беспилотным транспортом, изменении структуры и (или) конфигурации ее инфокоммуникаций.

4. Киберустойчивость системы контроля и управления БТС

Для оценки способности реагировать и противостоять угрозам кибербезопасности, поддерживать функциональность, определяемую как киберустойчивость. Устойчивая система должна снижать риски кибербезопасности и нейтрализовать негативные последствия кибератак.

Таким образом, *киберустойчивость* – это *способность компьютерной системы сохранять в установленных пределах значения параметров, характеризующих ее возможность выполнять свои функции в условиях компьютерных атак, не допускать несанкционированного доступа к информации и вычислительным ресурсам,*

нарушения целостности информации и доступности информационных сервисов.

Обсуждение и выводы

Состояние киберустойчивости не постоянно во времени. Кибератаки могут в любой момент оказать влияние на функционирование системы управления БТС.

Основная задача киберзащиты состоит в том, чтобы сохранять управляемость системой БТС. Это требует системного подхода к защите информации и инфраструктуры от киберугроз.

Для этого требуется четко определить угрозы кибербезопасности и систему их моделей для безопасного управления беспилотным транспортом. Что и сделано в статье.

Заключение

Принимая во внимание, что развитие беспилотного транспорта включено в приоритетные направления проектов технологического суверенитета страны, и формирование отрасли БТС носит опережающий характер, подчеркнем необходимость обеспечения полного контроля трафика БТС в границах зон социальных объектов, защищаемых объектов критической инфраструктуры, киберустойчивости БТС и защиты от их неправомерного применения, контроля выполнения маршрутных (полетных) заданий, выявления и предотвращения аномалий в поведении БТС, соответствия БТС законодательству РФ и требованиям регуляторов по безопасности их применения, для чего необходимо создание сети центров контроля и управления движением БТС, обеспечивающих ситуационную осведомленность и поддержку управленческих решений.

Список литературы

1. 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.

2. 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.

3. Скаридов А.С. К вопросу о детерминации морских автономных надводных средств применительно к правовому регулированию коммерческого судоходства // Океанский менеджмент. 2022. №1 (15). С.44-46.

4. Петрова Д.А., Губкина А.И. Захват американского беспилотного (автономного) подводного аппарата в Южно-Китайском море: правовые и политические аспекты // БГЖ. 2019. №4 (29). С. 375-377.

5. Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. № 1(47). С. 1–9.

6. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 4 (38). С. 39-42.

7. Основы кибербезопасности: Учебник. / Винокуров С.А., Минаев В.А., Поликарпов Е.С. и др. Воронеж-Москва: Воронежский институт МВД России, Московский университет МВД России им. В.Я. Кикотя, 2023. 392 с.

8. ГОСТ ISO/IEC 27100:2020. Информационная технология.

Кибербезопасность. Обзор и концепции. 24 с. Дата опубликования: 22.12.2020.

9. International Organization for Standardization, ISO/IEC 27000 – Information Security, ISO/IEC, 2022 // URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 04.04.2024).

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 20.03.2024

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: m1va@yandex.ru

Толпыгин Алексей Сергеевич – канд. техн. наук, доцент кафедры информационной безопасности, Московский государственный технический университет имени Н. Э. Баумана, e-mail: a.tolpygin@gmail.com

CYBER SECURITY AND CYBER SUSTAINABILITY UNMANNED TRANSPORT SYSTEMS

V.A. Minaev, A.S. Tolpygin

The article deals with the issues of ensuring cybersecurity of unmanned vehicles (UNV), characterizes the Russian features of its development, analyzes threats to cybersecurity to UNV control systems (CS), proposes an approach to the formation of actual threats at the stages of the life cycle of UNV CS– from the formation of initial requirements to the decommissioning of systems, considers the hierarchical structure of unmanned vehicles control and directions for the development of a system of cybersecurity threat models for unmanned vehicles – basic, particular and typical, an algorithm for the formation of a variety of threats to the cybersecurity of the UNV CS is given, threats to the control system are described depending on the level of vehicle autonomy. Special attention is paid to the application of artificial intelligence technologies in the UNV CS. It is concluded that the main task of cyber defense is to maintain the controllability of the system, which requires a system approach to protecting information and infrastructure of unmanned vehicles from cyber threats. In addition, there is a need for full control of UNV traffic within the boundaries of the zones of protected critical infrastructure facilities, protection against the misuse of UNV, control over the performance of route (flight) tasks, identification and prevention of anomalies in the behavior of UNV, compliance with Russian legislation and regulatory requirements for the safety of their use. To do this, it is necessary to create a network of UNV traffic control centers that provide situational awareness and support for management decisions.

Keywords: cybersecurity, cyber resilience, unmanned vehicles, artificial intelligence, threat models, information security.

Submitted 20.03.2024

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, Bauman Moscow State Technical University, Moscow, e-mail: a.tolpygin@gmail.com