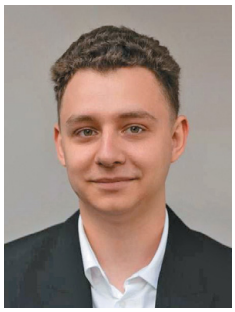
УДК 629.7.05:656.13:004.056
Оригинальная статья
https://doi.org/10.21683/1729-2646-2026-26-2-51-58

# Модель угроз БПЛА как составляющая модели угроз интеллектуальных транспортных систем

## UAV threat model as a component of the intelligent transportation systems threat model

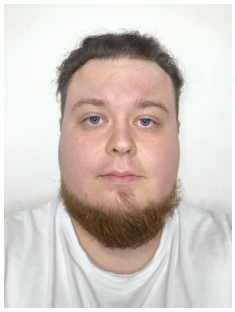
**Домашкин А.Д.[1], Логинова Л.Н.[1]*, Ковров А.И.[1]**
**Domashkin A.D.[1], Loginova L.N.[1]*, Kovrov A.I.[1]**

[1] *Российский университет транспорта, Москва, Российская Федерация*
[1] *Russian University of Transport, Moscow, Russian Federation*
* *ludmilanv@mail.ru*



*Домашкин А.Д.*

*Логинова Л.Н.*



*Ковров А.И.*

**Резюме. Цель.** *Беспилотные летательные аппараты (БПЛА) все шире интегрируются в интеллектуальные транспортные системы (ИТС), становясь одним из критических элементом транспортной инфраструктуры. Вместе с тем зависимость функционирования БПЛА от программного обеспечения (ПО), беспроводных каналов связи и внешних систем навигации делает их уязвимыми к информационным угрозам. Целью работы является проведение комплексного анализа угроз информационной безопасности (ИБ) БПЛА в контексте их функционирования в составе ИТС и разработка модели угроз, охватывающей аппаратные, программные, коммуникационные и инфраструктурные компоненты.* **Методы.** *В работе применены методы системного анализа, моделирования угроз ИБ, а также анализ архитектуры программно-аппаратных комплексов (ПАК) БПЛА с выделением ключевых объектов воздействия. Использованы подходы, основанные на классификации угроз по стандартам ФСТЭК РФ, а также методы анализа взаимосвязей между угрозами, уязвимостями и средствами защиты.* **Результаты.** *Разработана модель угроз БПЛА как элемента ИТС, охватывающая аппаратные компоненты, ПО, коммуникационные каналы, информационные потоки и наземную инфраструктуру. Выявлены наиболее критичные угрозы БПЛА, включая нарушение функционирования, компрометацию данных и физическое воздействие. Проведен анализ существующих решений по защите информации и показано, что отсутствует системный подход к обеспечению безопасности. На основе проведенного анализа обоснована необходимость внедрения методологии конструктивной информационной безопасности (КИБ) в соответствии с ГОСТ Р 72118-2025.* **Заключение.** *Предложенный подход, основанный на методологии КИБ, позволяет проектировать БПЛА с изначально заложенной устойчивостью к широкому спектру угроз ИБ, включая киберфизические атаки и нарушения целостности данных, что особенно актуально для интеграции БПЛА в ИТС, где отказ или компрометация одного элемента может повлечь системные сбои. Экспериментальная апробация подхода в рамках образовательных проектов подтверждает применимость и эффективность методологии КИБ.*

**Abstract. Aim**. *Unmanned aerial vehicles (UAVs) are increasingly integrated into intelligent transportation systems (ITS), becoming one of the critical elements of the transportation infrastructure. At the same time, the dependence of UAVs on software, wireless communication channels, and external navigation systems makes them vulnerable to cybersecurity threats. The purpose of the paper is to conduct a comprehensive analysis of cybersecurity threats to UAVs in the context of their operation as part of ITS and to develop a threat model covering hardware, software, communication, and infrastructure components.* **Methods**. *The paper uses methods of system analysis, cybersecurity threat modelling, as well as architecture analysis of UAV software and hardware systems involving the identification of key targets. The paper uses methods based on the classification of threats according to the standards of the FSTEC of the Russian Federation, as well as methods for analysing the relationships between threats, vulnerabilities, and means of protection.* **Results**. *A threat model of UAVs as an element of ITS has been developed, covering hardware components, software, communication channels, information flows, and ground infrastructure. The most critical threats have been identified, including disruption, data compromise, and physical impact. An analysis of existing information security solutions has been carried out and it has been shown that there is no systematic approach to ensuring security. Based on the analysis, the authors substantiate the application of the security by design (SBD) methodology according to GOST R 72118-2025.* **Conclusion**. *The proposed SBD-based approach allows designing UAVs with inherent resistance to a wide range of cybersecurity threats, including cyber-physical attacks and data integrity violations, which is especially important given the*

*requirements of UAV integration into ITS, where the failure or compromise of an element can lead to system failures. Experimental testing of the approach as part of educational projects confirms the applicability and effectiveness of the SBD methodology.*

**Ключевые слова:** *беспилотные летательные аппараты, информационная безопасность, интеллектуальные транспортные системы, модель угроз, конструктивная информационная безопасность, ГОСТ Р 72118-2025, программно-аппаратный комплекс, защита данных.*
**Keywords:** *unmanned aerial vehicles, information security, intelligent transportation systems, threat model, security by design, GOST R 72118-2025, hardware and software system, data protection.*

**Для цитирования:** *Домашкин А.Д., Логинова Л.Н., Ковров А.И. Модель угроз БПЛА как составляющая модели угроз интеллектуальных транспортных систем // Надежность. 2026. №2. С. 51-58. https://doi.org/10.21683/1729-2646-2026-26-2-51-58*
**For citation:** *Domashkin A.D., Loginova L.N., Kovrov A.I. UAV threat model as a component of the intelligent transportation systems threat model. Dependability 2026;2: 51-58. https://doi.org/10.21683/1729-2646-2026-26-2-51-58*

**Поступила:** *20.11.2025* / **После доработки:** *28.12.2025* / **К печати:** *25.05.2026*
**Received on:** *20.11.2025* / **Revised on:** *28.12.2025* / **For printing:** *25.05.2026*

## Введение

Обеспечение безопасности интеллектуальных транспортных систем (ИТС) в условиях стремительной цифровизации является актуально задачей. Интеграция, высокие темпы внедрения и уязвимости информационных и телекоммуникационных технологий, технологий искусственного интеллекта и связи влекут появление новых типов угроз безопасности ИТС [1–3]. В современном мире беспилотные летательные аппараты (БПЛА) стремительно распространяются в рамках ИТС [4, 5], значительно опережая развитие мер безопасности. БПЛА становятся критически важной частью транспортной системы, от стабильности которой зависит функционирование целых отраслей – от автоматизированных грузоперевозок до наблюдения за состоянием инфраструктуры. Из-за зависимости БПЛА от беспроводной связи, GPS, ГЛОНАСС и сложного программного обеспечения (ПО) они становятся привлекательной целью для злоумышленников.

Большинство современных исследований сосредоточены на отдельных технических уязвимостях, таких как GPS спуффинг, или на узконаправленных военных применениях, однако в данных исследованиях отсутствует комплексный подход, который рассматривает БПЛА не как отдельное устройство, а как часть интеллектуальной системы, включающей само устройство, наземные станции, операторов, цепочки поставок и т.д. Пробел в академическом подходе находит прямое отражение и в практической сфере. В частности, юридические исследования подтверждают наличие системных пробелов, указывая на отсутствие в российском законодательстве адекватных мер противодействия угрозам со стороны БПЛА [6].

В современной российской практике эксплуатации БПЛА отсутствуют унифицированные программные платформы, охватывающие обучение операторов, планирование и мониторинг полетов, анализ геопространственных данных, цифровую экспертизу, рейтинговую оценку участников и страхование, что обусловлено разнообразием отраслевых стандартов и технических ограничений, связанных с интеграцией разнородных систем. Данная ситуация обусловлена высокой специализацией задач, разнообразием отраслевых стандартов и технических ограничений, связанных с интеграцией разнородных систем. Вместе с тем, фрагментированный подход создает значительные риски информационной безопасности (ИБ), т.к. высокая специализация задач и сложность взаимодействия между различными системами затрудняют обеспечение единого уровня защиты данных и контроля доступа.

## 1. Состояние вопроса ИБ БПЛА

В статье [7] представлен иерархический подход к анализу рисков, включающий разработку многоуровневой модели угроз для БПЛА, которая охватывает общий анализ угроз на всем маршруте полета, кластерные модели для групп участков траектории и частные модели для отдельных сегментов маршрута. Упомянутый в [7] метод позволяет систематизировать угрозы по степени специфичности и масштабу воздействия, обеспечивая гибкость оценки рисков в зависимости от оперативной обстановки.

В работе [8] предложена модель угроз для БПЛА специального назначения, ориентированная на учет уникальных факторов, обусловленных высокой степенью конфиденциальности задач и критичности выполняемых функций; модель включает анализ уязвимостей, связанных с киберфизическими атаками, физическим захватом аппаратов и нарушением целостности данных в условиях противодействия.

Вместе с тем, для разработки комплексной модели угроз БПЛА как элемента ИТС необходимо учиты-

вать не только технические уязвимости, но и риски, связанные с нарушением логистических цепочек, киберфизическими атаками на инфраструктуру системы диспетчеризации, несанкционированным доступом к данным о маршрутах перемещения объектов транспортной системы. Архитектура БПЛА является программно-аппаратным комплексом (ПАК), состоящим из бортового компьютера, систем навигации и связи, модулей энергопитания, а также программного обеспечения (ПО) для планирования полетов, обработки данных и взаимодействия с внешними системами (рис. 1).

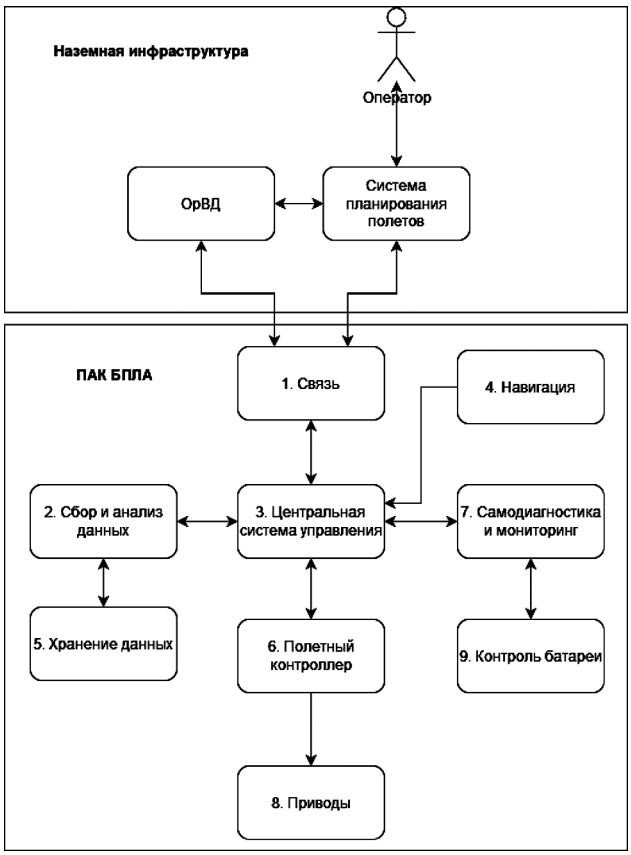



Рис. 1. Общая архитектура БПЛА

На основании рассмотренной архитектуры и проведенного анализа авторами разработана модель угроз БПЛА, выделены ключевые объекты воздействия, на которые могут быть направлены угрозы, а также возможные последствия реализованных угроз.

Далее перечислим все объекты воздействия, которые охватывают как внутренние компоненты БПЛА, так и внешние элементы взаимодействия с транспортной системой:

**1) Аппаратные компоненты БПЛА**

1.1) Бортовой компьютер и процессоры потенциально уязвимы к физическому повреждению, перехвату или изменению (модификации) при обслуживании.

1.2) Датчики (GPS, гироскопы, камеры) подвержены манипуляциями с данными (например, подмена GPS-координат, блокировка видеопотока).

1.3) Энергетическая система (аккумуляторы, двигатели) имеет риск перегрева, дистанционного отключения или физического разрушения.

**2) Программное обеспечение (ПО) БПЛА**

2.1) Алгоритмы автономного управления подвержены угрозам эксплуатации ошибок в ПО (например, ошибки в навигационных алгоритмах, уязвимости в системах обнаружения препятствий).

2.2) Операционная система подвержена внедрению вредоносного ПО или перезаписи подпрограмм для перехвата контроля управления.

2.3) Симуляторы и обучающие платформы обладают риском формирования у операторов навыков, не учитывающих реальные угрозы (например, игнорирование методов противодействия помехам связи).

**3) Коммуникационные каналы**

3.1) Радиоканалы связи с наземной станцией подвержены помехам, прослушиванию или перехвату сигнала.

3.2) Интеграция с внешними сетями (Wi-Fi, 4G/5G, спутниковые каналы) дает возможность осуществить MITM-атаку (man-in-the-middle), фишинг или использовать уязвимые протоколы передачи данных.

3.3) Интерфейсы API для взаимодействия с системами управления воздушным движением имеет риск несанкционированного доступа.

**4) Данные и информационные потоки**

4.1) Маршруты полета и траектории движения могут быть перехвачены или в них могут быть внесены изменения данных о координатах для отклонения БПЛА от курса.

4.2) Геоданные могут быть подделаны или удалены, что несет риск для логистики.

4.3) Персональные данные пассажиров/грузов подвержены риску утечки через возможные уязвимости в системах учета или облачных хранилищах.

**5) Наземная инфраструктура**

5.1) Наземные станции управления (НСУ) обладают уязвимостью к кибератакам (например, DDoS, компрометация серверов планирования полетов).

5.2) Системы организации воздушного движения (ОрВД) подвержены риску нарушения координации полетов из-за изменений в документации или аэронавигационной информации.

5.3) Сервисы страхования и рейтинговых оценок могут быть скомпрометированы и в них могут быть сфальсифицированы данных о состоянии БПЛА или репутации операторов.

Реализация угроз, связанных с эксплуатацией БПЛА, может повлечь за собой широкий спектр негативных последствий. С технической точки зрения возможна полная или частичная потеря управления воздушным судном, что может быть обусловлено как программными сбоями, так и физическим повреждением или выходом из строя критически важных компонентов бортового оборудования. Кроме того, нарушение целостности ПО, включая его несанкционированную модификацию или компрометацию, способно привести к некорректному

функционированию систем навигации, связи и управления. На операционном уровне реализация угрозы может спровоцировать срыв выполнения логистических задач, особенно в условиях высокой зависимости от автоматизированных доставок, что в свою очередь, может нарушить координацию воздушного движения, особенно в зонах интенсивного использования воздушного пространства, а также вызвать сбои в функционировании наземной инфраструктуры, включая системы управления полетами и пункты приема-передачи грузов. С юридической и регуляторной перспективы возникают риски несоблюдения нормативных требований, которые касаются обработки персональных и иных защищенных данных, что может повлечь административную или уголовную ответственность. В случае причинения физического ущерба – например, при падении БПЛА вследствие ошибки в ПО – возникает сложный вопрос о распределении ответственности между разработчиками, операторами, владельцами и регулирующими органами. Дополнительные правовые сложности могут быть связаны с компрометацией доказательственной базы, что затрудняет расследование инцидентов и установление причинно-следственных связей.

## 2. Разработка модели угроз БПЛА

Авторами разработана модель угроз БПЛА. В связи с тем, что модель угроз занимает большой объем, в статье приведен анализ модели угроз. Так, например, на рис. 2 представлены объекты воздействия, можно отметить, что наиболее часто подвергаемые угрозам объекты в соответствии с разработанной моделью, являются: О.1-Автоматизированное рабочее место оператора, О.2-Сервер, О.3-Периферийное оборудование, О.6-Активное сетевое оборудование (далее по тексту используются названия объектов, угроз и средств защиты в соответствии с классификацией ФСТЭК[1]).

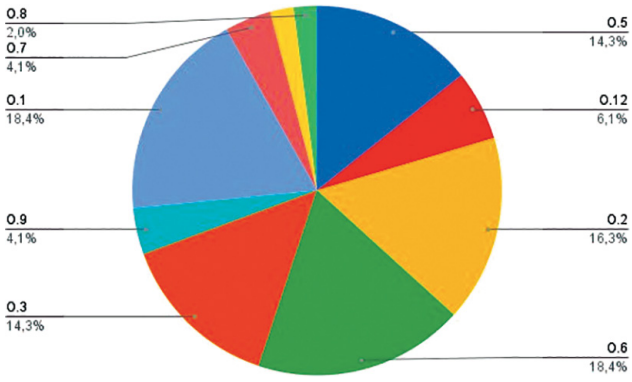



Рис. 2. Диаграмма распределения объектов воздействия, рассмотренных в разработанной модели угроз БПЛА

Угрозы ИБ, рассмотренные в разработанной модели, приведены на рис. 3, можно отметить, что УБИ.8[2] – Угроза нарушения функционирования (работоспособности) наиболее встречающийся вид угроз, дополнительно критичными являются угрозы, воздействующие на коммуникационные каналы, целостность данных и физическую безопасность БПЛА, т.к. они способны нарушить функционирование всей транспортной системы.

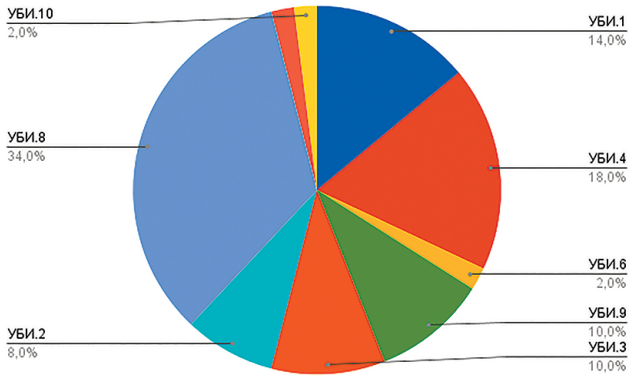



Рис. 3. Диаграмма распределения угроз ИБ, представленных в разработанной модели

Анализируя модель угроз, авторы провели анализ типов ПО, которое чаще всего встречается для защиты от угроз ИБ при использовании БПЛА. При построении модели угроз авторами было рассмотрено более 60-ти программных продуктов, которые могут быть использованы для защиты. Все рассмотренные продукты были классифицированы по типам, на рис. 4 представлена диаграмма распределения типа рассмотренного ПО. Следует отметить, что для предотвращения угроз чаще всего применяется физические способы защиты, внедрение методов управления уязвимостями, применение шифрования данных и также применение систем аутентификации и авторизации пользователей.


Рис. 4. Диаграмма распределения ПО для защиты от угроз, представленных в разработанной модели

На рис. 5 представлена схема взаимоотношения угроз, объектов и средств защиты ИБ, на которой показано, что отсутствует комплексная система защиты, что увеличивает общее количество уязвимостей ИТС при использовании БПЛА в случае выполнении соответствующего функционала.

[1] URL: https://bdu.fstec.ru/threat-section/threats
[2] URL: https://bdu.fstec.ru/threat-section/threats

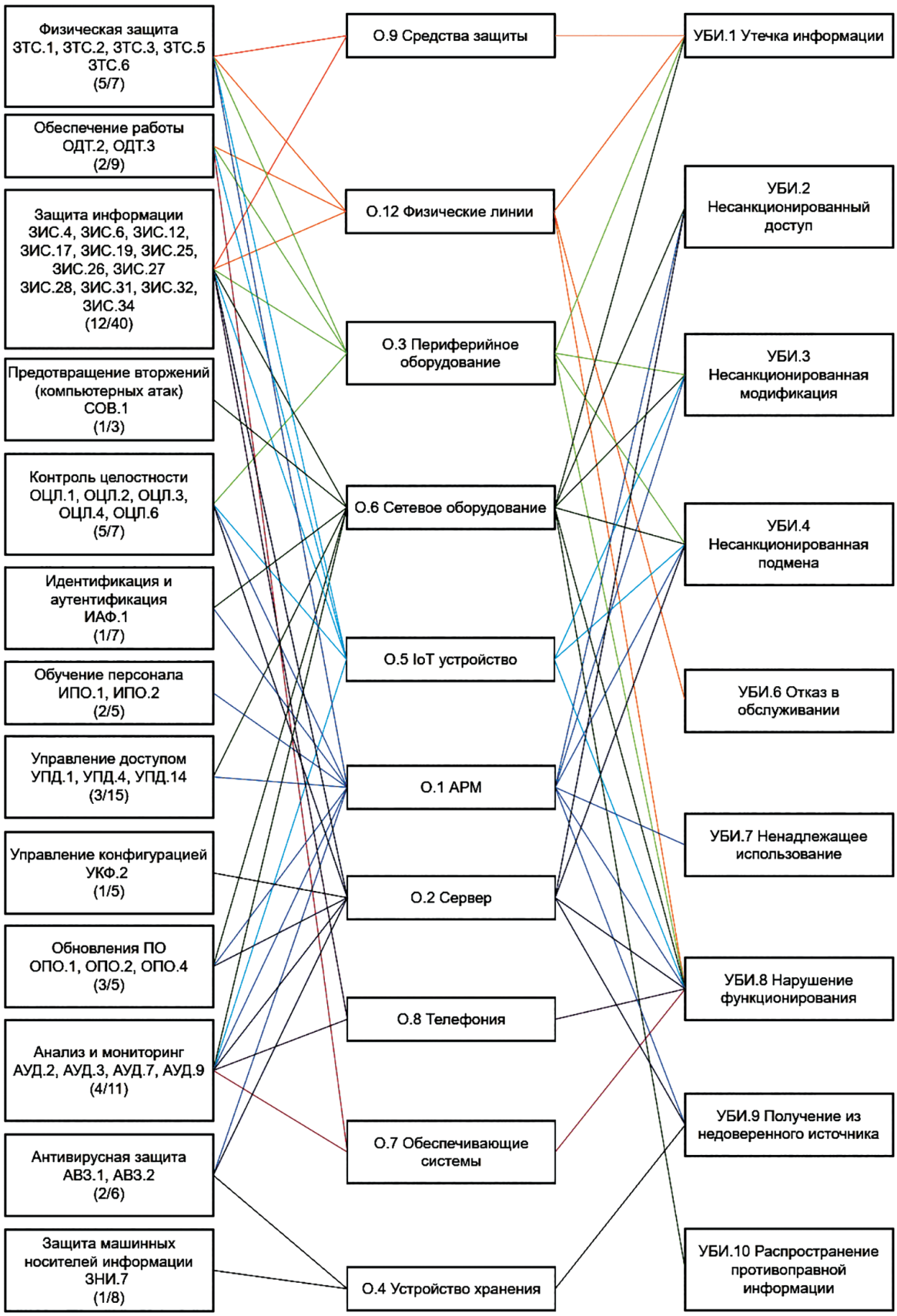



Рис. 5. Схема взаимоотношения угроз, объектов и средств защиты ИБ[1]

[1] URL: https://bdu.fstec.ru/threat-section

## 3. Конструктивная информационная безопасность

Указанные недостатки свидетельствуют о необходимости перехода от традиционных подходов к проактивной защите, встроенной в архитектуру системы модели безопасности. В качестве такого решения в последние годы активно развивается концепция кибериммунитета, предложенная «Лабораторией Касперского», которая легла в основу формирования отечественного подхода к проектированию систем, устойчивых к угрозам ИБ. Ключевые принципы концепции были систематизированы и стандартизированы в рамках национального документа ГОСТ Р 72118-2025 «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки» (КИБ) [9].

Стандарт разработан ФСТЭК, «Лаборатория Касперского» и ИСП РАН – группа ключевых носителей практики в области ИБ. Проектирование и конструирование защищенного БПЛА, применимого в ИТС, возможно на основе методологии разработки систем с КИБ, при этом упомянутый принцип позволяет создавать ПАК, которые не только устойчивы к внешним и внутренним угрозам, но и способны быстро восстанавливаться после возможных сбоев.

На кафедре «Управление и защита информации» накоплен значительный опыт разработки систем с КИБ. Так, например, студенты кафедры с 2022-23 годы участвовали в первом и втором хакатоне Лаборатории Касперского, посвященному КИБ [10], в 2023 году выпускник кафедры в составе команды *GenericBoys* разработал архитектуру и прототип конструктивно защищенного БПЛА для мониторинга трубопроводов, которая получила первое место на хакатоне по Киберимунной разработке [11]. Студенты кафедры и преподаватели регулярно участвуют в соревнованиях по кибериммунитету, так, например, команда студентов под руководством Логиновой Л.Н. участвовала в 2024-2025 гг. в инженерных соревнованиях в компетенции «Кибериммунная автономность» в рамках проектно-образовательного интенсива Архипелаг, посвященный проектированию БАС [12]. На кафедре «Управление и защита информации» РУТ(МИИТ) Домашкиным А.Д. была успешно защищена первая дипломная работа в 2023 г. на тему «Разработка методики внедрения кибериммунного подхода в решении задач информационной безопасности в транспортной отрасли [13], после этого тематика КИБ стала популярной для рассмотрения в дипломных проектах.

## Заключение

На основе накопленного опыта и успешно выполненных задач авторы предлагают в дальнейшем использовать методологию КИБ для проектирования архитектуры безопасного БПЛА, предназначенного для интеграции в ИТС. Данный подход позволит заложить свойства КИБ на ранних этапах жизненного цикла разработки – от анализа требований и моделирования угроз до проектирования аппаратно-программных компонентов и механизмов самодиагностики. Использование стандарта ГОСТ Р 72118-2025 в сочетании с практиками, апробированными в ходе хакатонов и проектно-образовательных инициатив, обеспечит создание БПЛА, способного не только противостоять целенаправленным атакам, но и сохранять функциональность в условиях неопределенности и динамически изменяющихся угроз, что особенно критично для транспортной инфраструктуры.

**Благодарности.** Работа выполнена за счет бюджетного финансирования в рамках государственного задания от 20.03.2025 № 103-00001-25-02.

## Список литературы

1. Розенберг И.Н. Методы и алгоритмы создания интеллектуальных геоинформационных систем для управления транспортными процессами / И.Н. Розенберг, С.Л. Беляков, А.В. Боженюк [и др.]; под ред. И.Н. Розенберга. М.: ВИНИТИ РАН, 2019. 289 с.

2. Шубинский И.Б. Надежность, риски, безопасность систем управления на железнодорожном транспорте: монография / И.Б. Шубинский, Е.Н. Розенберг, А.В. Бочков. М., Вологда: Инфра – Инженерия, 2024. 416 с.

3. Баранов Л.А. Моделирование и оценка рисков безопасности интеллектуальных систем водного транспорта / Л.А. Баранов, Н.Д. Иванова, И.Ф. Михалевич // Автоматика на транспорте. 2025. Т. 11. № 1. С. 7-15. DOI: 10.20295/2412-9186-2025-11-01-7-15 EDN FBRTKV. URL: https://www.elibrary.ru/item.asp?id=80472960

4. Использование беспилотных летательных средств: опыт, перспективы, проблемы / А.Д. Домашкин, Л.Н. Логинова, А.И. Ковров [и др.] // Интеллектуальные транспортные системы: Материалы IV Международной научно-практической конференции, Москва, 22 мая 2025 года. М.: Российский университет транспорта (МИИТ), 2025. С. 517-525. DOI 10.30932/9785002587582-2025-517-525 EDN HIIYVX.

5. Баранов Л.А., Сафронов А.И., Сидоренко В.Г Развитие интеллектуальных систем управления электрическим транспортом Автоматика, связь, информатика. 2025. № 10. С. 30–32.

6. Зайкова С.Н., Виноградский Д.Д. Беспилотные транспортные средства (аппараты) как угроза транспортной безопасности // Вестник СГЮА. 2024. №1(156). URL: https://cyberleninka.ru/article/n/bespilotnye-transportnye-sredstva-apparaty-kak-ugroza-transportnoy-bezopasnosti (дата обращения: 23.03.2025).

7. Аралбаев Т.З., Галимов Р.Р., Гетьман М.А. и др. Иерархический анализ рисков моделей угроз беспилотных

летательных аппаратов // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2023. № 2. URL: https://cyberleninka.ru/article/n/ierarhicheskiy-analiz-riskov-modeley-ugroz-bespilotnyh-letatelnyh-apparatov (дата обращения: 16.07.2025).

8. Винокуров А.В. Анализ уязвимостей комплексов с беспилотными летательными аппаратами и классификация угроз безопасности циркулирующей в них информации // I-methods. 2016. № 1. URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-kompleksov-s-bespilotnymi-letatelnymi-apparatami-i-klassifikatsiya-ugroz-bezopasnosti-tsirkuliruyuschey-v-nih (дата обращения: 11.10.2025).

9. ГОСТ Р 72118-2025 Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки. М.: Российский институт стандартизации, 2025. IV, 45 с.

10. Повышение HardSkill с помощью соревнований по CTF / Л.Н. Логинова, Р.А. Бобков, С.А. Костенко [и др.] // Интеллектуальные транспортные системы: Материалы II Международной научно-практической конференции, Москва, 25 мая 2023 года. М.: Российский университет транспорта, 2023. С. 789-793. DOI 10.30932/9785002182794-2023-789-793 EDN DTKGRL.

11. Как прошел хакатон «Лаборатории Касперского» по проектированию дронов. URL: https://codenrock.com/blog/kak-proshel-hakaton-laboratorii-kasperskogo-po-proektirovaniyu-dronov/ (дата обращения: 11.08.2025).

12. Логинова Л.Н., Галыба Л.Д., Степанов Д.Е. Командный дух и инновации: участие в хакатоне по киберимунной автономности// Интеллектуальные транспортные системы: Материалы IV Международной научно-практической конференции, Москва, 22 мая 2025 года. М.: Российский университет транспорта, 2025. С. 878-886.

13. Логинова Л.Н., Домашкин А.Д. Применение принципов кибериммунитета для обеспечения безопасности в транспортных системах // Интеллектуальные транспортные системы: Материалы III Международной научно-практической конференции, Москва, 30 мая 2024 года. М.: Российский университет транспорта (МИИТ), 2024. С. 645-649. DOI 10.30932/9785002446094-2024-645-649 EDN HCNJYS.

## References

1. Rozenberg I.N., Belyakov S.L., Bozhenyuk A.V. et al. Rozenberg I.N., editor. [Methods and algorithms for creating intelligent geographic information systems for transportation process management]. Moscow: VINITI RAS; 2019. (in Russ.)

2. Shubinsky I.B., Rozenberg E.N, Bochkov A.V. [Dependability, risks, safety of control systems in railway transportation: a monograph]. Vologda: Infra–Engineering; 2024. (in Russ.)

3. Baranov L.A., Ivanova N.D., Mihalevich I.F. Modelling and Assessment of Security Risks of Intelligent Water Transport Systems. *Transport automation research* 2025;1:7-15. (in Russ.) DOI: 10.20295/2412-9186-2025-11-01-7-15 EDN FBRTKV. Available at: https://www.elibrary.ru/item.asp?id=80472960.

4. Domashkin A.D., Loginova L.N., Kovrov A.I. et al. [Use of unmanned aerial vehicles: experience, prospects, problems]. In: [Intelligent transportation systems: Proceedings of the IV International science and practice conference]. Moscow; May 22, 2025. Moscow: Russian University of Transport (MIIT); 2025. Pp. 517-525. (in Russ.) DOI 10.30932/9785002587582-2025-517-525 EDN HIIYVX.

5. Baranov L.A., Safronov A.I., Sidorenko V.G. Development of Intelligent Control Systems for Electric Transport. *Automation, communications, informatics* 2025;10:30-32. (in Russ.)

6. Zaikova S.N., Vinogradsky D.D. Unmanned vehicles (airships) as a threat to transportation security. (accessed: 23.03.2025). *SSLA Bulletin* 2024;1(56). Available at: https://cyberleninka.ru/article/n/bespilotnye-transportnye-sredstva-apparaty-kak-ugroza-transportnoy-bezopasnosti. (in Russ.)

7. Aralbaev T.Z., Galimov R.R., Getman M.A. et al. Hierarchical risk analysis of unmanned aerial vehicle threat models. *Izvestiya of Saratov University. Mathematics. Mechanics. Informatics* 2023;23(2):241-252. (accessed: 16.07.2025). Available at: https://cyberleninka.ru/article/n/ierarhicheskiy-analiz-riskov-modeley-ugroz-bespilotnyh-letatelnyh-apparatov. (in Russ.)

8. Vinokurov A.V. Vulnerability analysis complexes with unmanned aerial vehicles and classification of security threats circulating information in them. *I-methods* 2016;1. (accessed: 11.10.2025). Available at: https://cyberleninka.ru/article/n/analiz-uyazvimostey-kompleksov-s-bespilotnymi-letatelnymi-apparatami-i-klassifikatsiya-ugroz-bezopasnosti-tsirkuliruyuschey-v-nih. (in Russ.)

9. GOST R 72118-2025. Information protection. Systems secure by design. Development methodology. Moscow: Russian Standardization Institute; 2025. (in Russ.)

10. Loginova L.N., Bobkov R.A., Kostenko S.A. et al. [Improving Hard Skills through CTF competitions]. In: [Intelligent transportation systems: Proceedings of the II International science and practice conference]. Moscow; May 25, 2023. Moscow: Russian University of Transport (MIIT); 2023. Pp. 789-793. (in Russ.) DOI 10.30932/9785002182794-2023-789-793 EDN DTKGRL.

11. How was Kaspersky Lab's drone design hackathon. (accessed: 11.08.2025). Available at: https://codenrock.com/blog/kak-proshel-hakaton-laboratorii-kasperskogo-po-proektirovaniyu-dronov/. (in Russ.)

12. Loginova L.N., Galyba L.D., Stepanov D.E. [Team spirit and innovation: participation in the hackathon on cyberimmune autonomy]. In: [Intelligent transportation systems: Proceedings of the IV International science and

practice conference]. Moscow; May 22, 2025. Moscow: Russian University of Transport; 2025. Pp. 878-886. (in Russ.)

13. Loginova L.N., Domashkin A.D. [Applying cyberimmunity principles to ensure security in transportation systems]. In: [Intelligent transportation systems: Proceedings of the III International science and practice conference]. Moscow; May 30, 2024. Moscow: Russian University of Transport (MIIT); 2024. Pp. 645-649. DOI 10.30932/9785002446094-2024-645-649 EDN HCNJYS. (in Russ.)

## Сведения об авторах

**Домашкин Алексей Дмитриевич** (Aleksey D/ Domashkin) – аспирант кафедры «Управление и защита информации», Российский университет транспорта (Russian University of Transport (MIIT)), Российская Федерация, Москва, e-mail: mail@adomashkin.ru

**Логинова Людмила Николаевна** (Lyudmila N/ Loginova) – кандидат технических наук, доцент, доцент кафедры «Управление и защита информации», Российский университет транспорта (Russian University of Transport (MIIT)), Российская Федерация, Москва, e-mail: ludmilanv@mail.ru

**Ковров Артем Игоревич** (Artiom I/ Kovrov) – студент кафедры «Управление и защита информации», Российский университет транспорта (Russian University of Transport (MIIT)), Российская Федерация, Москва, e-mail: kovrov_tema@mail.ru

## About the authors

**Alexey D. Domashkin,** Postgraduate Student, Department of Information Management and Protection, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: mail@adomashkin.ru.

**Lyudmila N. Loginova,** Candidate of Engineering, Associate Professor, Senior Lecturer, Department of Information Management and Protection, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: ludmilanv@mail.ru .

**Artyom I. Kovrov,** Student, Department of Information Management and Protection, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: kovrov_tema@mail.ru.

## Вклад авторов в статью

**Домашкин А.Д.** – разработка модели угроз БПЛА как элемента ИТС, охватывающая аппаратные компоненты, ПО, коммуникационные каналы, информационные потоки и наземную инфраструктуру.

**Логинова Л.Н.** – анализ архитектуры ПАК БПЛА с выделением ключевых объектов воздействия.

**Ковров А.И.** – выявление наиболее критичных угроз БПЛА, включая нарушение функционирования, компрометацию данных и физическое воздействие.

## Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.