ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№2
2026

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

2 (358)

APRIL – JUNE 2026

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).
Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.
Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*
Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

COMPUTER SCIENCE

МАЗМҰНЫ

КОМПЬЮТЕРЛІК ҒЫЛЫМДАР

СОДЕРЖАНИЕ

КОМПЬЮТЕРНЫЕ НАУКИ

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 2.
Namber 358 (2026). 391–413

https://doi.org/10.32014/2026.2518-1726.445

IRSTI 28.17.23
UDC 629.7.052:004.056

**© Tursunbayeva G.U.*, Satybaldina D.Zh., Tleuberdin S.T.,
Tashatov N.N., Egamberdiyev E.E., 2026.**
Research Institute of Information Security and Cryptology, L.N. Gumilyov
Eurasian National University, Astana, Kazakhstan.
E-mail: t.gulzhamal@outlook.com

ANOMALY DETECTION IN UAV TELEMETRY SYSTEMS BASED ON SIMULATION MODELING

Tursunbayeva Gulzhamal — PhD Student in Information Security System, Junior Researcher at the Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: t.gulzhamal@outlook.com, https://orcid.org/0000-0002-2044-8027;
Satybaldina Dina — Candidate of Physical and Mathematical Sciences, Professor, Head of Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: satybaldina_dzh@enu.kz, https://orcid.org/0000-0003-0291-4685;
Tleuberdin Saken — PhD Student in Information Security System, Junior Researcher at the Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: sakentleuberdin@gmail.com, https://orcid.org/0000-0001-9170-9936;
Tashatov Nurlan — Candidate of Physical and Mathematical Sciences, Researcher of Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: tashatov_nn@enu.kz, https://orcid.org/0000-0002-3271-2163;
Egamberdiyev Eldor — PhD, Researcher of Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: eeldoru@gmail.com, https://orcid.org/0000-0001-5289-6580.

Abstract. Currently, the rapid development and widespread implementation of unmanned technologies have led to significant changes in various fields of human activity. At the same time, the risks associated with the unauthorized use of aircraft systems have increased. This has resulted in the emergence of a separate research area focused on the protection and counteraction of various components and platforms of aerial systems. Despite the existence of modern attack and anomaly detection methods, their effectiveness is significantly reduced under complex operating scenarios, including dynamically changing environments, interference

effects, small target sizes, and low radar visibility. To address this issue, this study presents the main results of a comprehensive analysis of modern cyber threats and vulnerabilities arising in unmanned aerial vehicle (UAV) systems. Based on the analysis, an up-to-date classification of existing attack types targeting the basic UAV architecture was developed. This made it possible to investigate the main protection methods for ensuring the security of UAV systems and components, as well as to classify cyberattack detection methods for these systems. Based on the obtained data, a multi-level protection architecture was developed, including three main levels: a secure communication channel, a secure flight controller, and a secure ground control station. The developed software environment for telemetry stream simulation in Python 3.12 enabled the generation of MAVLink/UDP/TCP packets, as well as the emulation of attacks and detection of network anomalies in UAV telemetry systems. The obtained results include the processing of 97 MAVLink packets, where the anomaly injection rate amounted to 10% with a total of 118 anomalies detected. The average MAVLink packet delay was 0.037 seconds, indicating stable operation of the telemetry channel. Experimental verification consisting of 100 cycles demonstrated the ability to detect packet structure violations, false identifiers, coordinate substitution, and delay anomalies.

Keywords: unmanned aerial vehicles (UAVs); telemetry channel; UAV cybersecurity; anomaly detection; MAVLink; attacks; vulnerability

For citations: Tursunbayeva G.U., Satybaldina D.Zh., Tleuberdin S.T., Tashatov N.N., Egamberdiyev E.E. Anomaly detection in uav telemetry systems based on simulation modeling. Academic Scientific Journal of Computer Science, 2026. — No.2. – P. 391-413. DOI https://doi.org/10.32014/2026.2518-1726.445*

«Ақпараттық қауіпсіздік және криптология» ғылыми-зерттеу институты,
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
E-mail: t.gulzhamal@outlook.com

СИМУЛЯЦИЯЛЫҚ МОДЕЛЬДЕУ НЕГІЗІНДЕ ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫНЫҢ ТЕЛЕМЕТРИЯЛЫҚ ЖҮЙЕЛЕРІНДЕГІ АНОМАЛИЯЛАРДЫ АНЫҚТАУ

Турсунбаева Гулжамал — Ақпараттық қауіпсіздік жүйелері білім беру бағдарламасының докторанты, «Ақпараттық қауіпсіздік және криптология» ғылыми-зерттеу институтының кіші ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, E-mail: t.gulzhamal@outlook.com, https://orcid.org/0000-0002-2044-8027;

Сатыбалдина Дина — физика-математика ғылымдарының кандидаты, профессор, «Ақпараттық қауіпсіздік және криптология» ғылыми-зерттеу институтының директоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: satybaldina_dzh@enu.kz, https://orcid.org/0000-0003-0291-4685;

Тлеубердин Сакен — Ақпараттық қауіпсіздік жүйелері білім беру бағдарламасының докторанты, «Ақпараттық қауіпсіздік және криптология» ғылыми-зерттеу институтының кіші ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, E-mail: sakentleuberdin@gmail.com, https://orcid.org/0000-0001-9170-9936;
Ташатов Нурлан — физика-математика ғылымдарының кандидаты, доцент, «Ақпараттық қауіпсіздік және криптология» ғылыми-зерттеу институтының ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: tashatov_nn@enu.kz, https://orcid.org/0000-0002-3271-2163;
Эгамбердиев Эльдор — PhD, «Ақпараттық қауіпсіздік және криптология» ғылыми-зерттеу институтының ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: eeldoru@gmail.com, https://orcid.org/0000-0001-5289-6580.

Аннотация. Қазіргі уақытта ұшқышсыз технологиялардың қарқынды дамуы мен кеңінен енгізілуі адам қызметінің әртүрлі салаларында елеулі өзгерістерге алып келді. Сонымен қатар ұшу аппараттары жүйелерін рұқсатсыз пайдалануға байланысты тәуекелдер де артты. Бұл ұшу жүйелерінің әртүрлі компоненттері мен платформаларын қорғау және қарсы әрекет ету саласында жеке ғылыми бағыттың қалыптасуына себеп болды. Қолданыстағы шабуылдар мен аномалияларды анықтау әдістерінің болуына қарамастан, олардың тиімділігі динамикалық өзгеретін орта, кедергілердің әсері, нысандардың шағын өлшемдері және төмен радиолокациялық байқалуы сияқты күрделі пайдалану сценарийлерінде айтарлықтай төмендейді. Осы мәселені шешу мақсатында зерттеуде ұшқышсыз ұшу аппараттары (ҰҰА) жүйелерінде туындайтын заманауи киберқауіптер мен осалдықтарды кешенді талдау нәтижелері ұсынылған. Талдау негізінде ҰҰА базалық архитектурасына бағытталған шабуылдардың өзекті жіктемесі жасалды. Бұл ҰҰА жүйелері мен компоненттерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеуге, сондай-ақ олардың жүйелеріне бағытталған кибершабуылдарды анықтау тәсілдерін жіктеуге мүмкіндік берді. Алынған мәліметтер негізінде қорғалған байланыс арнасын, қорғалған ұшу контроллерін және қорғалған жерүсті басқару станциясын қамтитын көпдеңгейлі қорғаныс архитектурасы әзірленді. Python 3.12 ортасында жасалған телеметриялық ағындарды модельдеу бағдарламалық ортасы MAVLink/UDP/TCP форматындағы пакеттерді генерациялауға, шабуылдарды имитациялауға және ҰҰА телеметрия жүйесіндегі желілік аномалияларды тіркеуге мүмкіндік берді. Алынған нәтижелерге сәйкес 97 MAVLink пакеті өңделді, мұнда аномалия инъекцияларының үлесі 10%-ды, ал олардың жалпы саны 118 бірлікті құрады. MAVLink пакетінің орташа кідіріс уақыты 0,037 секундты құрады, бұл телеметриялық арнаның тұрақты жұмысын көрсетеді. 100 циклден тұратын эксперименттік верификация деректер пакеттері құрылымының бұзылуын, жалған идентификаторларды, координаталарды алмастыруды және кідіріс аномалияларын анықтау мүмкіндігін көрсетті.

Түйін сөздер: ұшқышсыз ұшу аппараттары (ҰҰА); телеметрия арнасы;

ҰҰА киберқорғанысы; аномалияларды анықтау; MAVLink; шабуылдар; осалдық

©Турсунбаева Г.*, Сатыбалдина Д., Тлеубердин С., Ташатов Н., Эгамбердиев Э., 2026.
НИИ информационной безопасности и криптологии Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан.
E-mail: t.gulzhamal@outlook.com

ОБНАРУЖЕНИЕ АНОМАЛИЙ В ТЕЛЕМЕТРИЧЕСКИХ СИСТЕМАХ БПЛА НА ОСНОВЕ СИММУЛЯЦИОННОГО МОДЕЛИРОВАНИЯ

Турсунбаева Гулжамал — докторант образовательной программы «Системы информационной безопасности», младший научный сотрудник НИИ информационной безопасности и криптологии, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,
E-mail: t.gulzhamal@outlook.com, https://orcid.org/0000-0002-2044-8027;
Сатыбалдина Дина — кандидат физико-математических наук, профессор, директор НИИ информационной безопасности и криптологии, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,
E-mail: satybaldina_dzh@enu.kz, https://orcid.org/0000-0003-0291-4685;
Тлеубердин Сакен — докторант образовательной программы «Системы информационной безопасности», младший научный сотрудник НИИ информационной безопасности и криптологии, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,
E-mail: sakentleuberdin@gmail.com, https://orcid.org/0000-0001-9170-9936;
Ташатов Нурлан — кандидат физико-математических наук, доцент, научный сотрудник НИИ информационной безопасности и криптологии, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,
E-mail: tashatov_nn@enu.kz, https://orcid.org/0000-0002-3271-2163;
Эгамбердиев Эльдор — PhD, научный сотрудник НИИ информационной безопасности и криптологии, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан,
E-mail: eeldoru@gmail.com, https://orcid.org/0000-0001-5289-6580.

Аннотация. *Актуальность.* Стремительное развитие и широкое внедрение беспилотных технологий привели к значительным изменениям в различных сферах деятельности человека. Одновременно возросли риски, связанные с несанкционированным использованием беспилотных летательных аппаратов и нарушением работы их телеметрических систем. Это обусловило формирование отдельного направления исследований, связанного с противодействием киберугрозам и защитой компонентов, каналов связи и платформ БПЛА. Несмотря на наличие существующих методов обнаружения атак и аномалий, их эффективность может снижаться в условиях сложных сценариев эксплуатации, включая динамически изменяющуюся среду, помеховое воздействие, малые размеры целей и низкую радиолокационную заметность. *Цель.* Разработать и апробировать

подход к обнаружению аномалий в телеметрических системах БПЛА на основе симуляционного моделирования телеметрических потоков, имитации атак и анализа сетевых аномалий. *Методы.* В исследовании проведен комплексный анализ современных киберугроз и уязвимостей, возникающих в системах беспилотных летательных аппаратов. На основе анализа составлена классификация существующих типов атак на базовую архитектуру БПЛА, что позволило определить основные методы защиты систем и компонентов БПЛА, а также классифицировать подходы к обнаружению кибератак. На основе полученных данных разработана многоуровневая архитектура защиты, включающая три основных уровня: защищенный канал связи, защищенный контроллер полета и защищенную наземную контрольную станцию. Для экспериментальной проверки создана программная среда моделирования телеметрических потоков на Python 3.12, позволяющая генерировать пакеты в формате MAVLink/UDP/TCP, имитировать атаки и фиксировать сетевые аномалии в системе телеметрии БПЛА. *Результаты и выводы.* Полученные результаты включают обработку 97 пакетов MAVLink, при этом доля инъекций аномалий составила 10%, а общее количество зафиксированных событий достигло 118 единиц. Среднее время задержки пакета MAVLink составило 0,037 секунды, что свидетельствует о стабильной работе телеметрического канала в условиях моделирования. Экспериментальная верификация, состоящая из 100 циклов, продемонстрировала способность предложенного подхода обнаруживать нарушения структуры пакетов данных, ложные идентификаторы, подстановку координат и аномалии задержек. Практическая значимость исследования заключается в возможности использования разработанной симуляционной среды и многоуровневой архитектуры защиты при проектировании систем кибербезопасности БПЛА, мониторинге телеметрических каналов и разработке средств обнаружения атак на беспилотные платформы.

Ключевые слова: беспилотные летательные аппараты, БПЛА, канал телеметрии, киберзащита БПЛА, обнаружение аномалий, MAVLink, UDP, TCP, атаки, уязвимости, симуляционное моделирование.

Финансирование: *Данное исследование было профинансировано Комитетом науки Министерства науки и высшего образования Республики Казахстан в рамках реализации проекта ГФ (ИРН: AP26101065).*

Введение. На сегодняшний день широкое применение беспилотных летательных аппаратов (БПЛА) для коммерческих, гражданских и военных целях значительно повысило потребность безопасности их систем, механизмов и компонентов (Islam et al., 2025). Учитывая, что они все чаще используются в выполнении самых разнообразных задачах начиная от инспекции инфраструктуры, аэрофотосъемки, мониторинг окружающей среды, дистанционного зондирования Земли (ДЗЗ) и до доставки посылок в

труднодоступные места делают их крайне уязвимыми для кибервторжений. Эти угрозы могут нарушить выполнение различных миссий и поставить под угрозу целостность данных, включая причинение физического вреда БПЛА (Alsumayt et al., 2026). По мере расширения масштабов и усложнения задач и миссий в различных секторах, растущая зависимость от цифровых платформ и систем подвергает их воздействию широкого спектра угроз кибербезопасности.

Операционная целостность платформы БПЛА напрямую зависит от безопасности базовых подсистем, таких как телеметрическая связь, каналы управления и контроля, навигация на основе GNSS/GPS, механизмы удалённой идентификации, облачные сервисы мониторинга и хранения данных (Tlili et al., 2024).

Структурная схема базовой архитектуры БПЛА состоит из трех основных компонентов:

1. Бортовой сегмент БПЛА обеспечивает автономное функционирование БПЛА в воздушном пространстве. В данном блоке реализация алгоритмов автоматического управления непосредственно выполняются в подсистеме Flight Controller, а для определения координат, скорости и высоты воздушного пространства применяется подсистема Navigation System. Передача телеметрических данных и приём управляющих команд по заданному каналу обеспечивается через подсистему Communication Module. Для выполнения различных миссий БПЛА может в составе иметь Payload. Питание всех бортовых компонентов БПЛА и поддержание их стабильной работы в режиме реального времени обеспечивается через подсистему Power System.

2. Наземная система управления БПЛА обеспечивает планирование заданной миссии, мониторинг и контроль параметров телеметрии, включая командное управление БПЛА.

3. Облачная платформа БПЛА предназначена для обработки и хранения данных.

Связь между БПЛА и наземной станцией осуществляется посредством радиоканала или сотовой сети с использованием протоколов передачи данных. Обмен данными между наземной системой управления БПЛА и облачной платформой осуществляется через сеть Интернет.

Нарушение функциональности любого из них может привести к потере устойчивости управления полетом БПЛА в воздушном пространстве, снижению точности навигационных решений и полной потере связи с наземной станцией что в конечном итоге повышает вероятность возникновения аварийных ситуаций и создаёт риск невыполнения поставленной миссии.

По своей природе, БПЛА являются более уязвимы к атакам, чем пилотируемые летательные аппараты. Причиной тому является отсутствие вмешательства человека, включая сильную зависимость от беспроводной связи и наличие не защищенной аппаратной архитектуры. В настоящее время наиболее распространены атаки, осуществляемые с четырёх сторон: датчики

БПЛА, связь, программное обеспечение и кибербезопасность. Типовые кибератаки на БПЛА охватывают каналы связи, навигационную подсистему, полётный контроллер, полезную нагрузку, энергетическую систему и наземно-облачную инфраструктуру, формируя многоуровневую поверхность атак, что повышает актуальность разработки подходящих решений для обеспечения безопасности БПЛА.

Целью исследования является формирование концептуальной модели многоуровневой системы киберзащиты БПЛА и её программная реализация в виде симуляционной платформы, предназначенной для моделирования телеметрического обмена, инъекции аномалий и оценки эффективности детектирования нарушений целостности, аутентичности и непрерывности передачи данных без использования методов машинного обучения.

Обзор литературы. Разработка подходящих оптимальных решений для обеспечения безопасности БПЛА затруднена из-за множества факторов (Alshamrani et al., 2026).Самым распространённым из них можно отметить крайне ограниченную вычислительную мощность на борту БПЛА (Mohammed et al., 2025). Это ограничивает возможности внедрения программного обеспечения и их компонентов для обеспечения безопасности и целостности передаваемых данных. Более того наземные станции управления БПЛА часто представляют собой простых устройств дистанционного управления, которые имеют ограничения в установке дополнительных программных функций безопасности (Burbank et al., 2026).Проблемы, связанные с ограничениями по размеру, весу БПЛА делают многие аппаратные решения для обеспечения безопасности непрактичными. В том числе многие механизмы безопасности, разработанные для традиционных компьютерных систем и сетей передачи данных, не могут быть напрямую применены к БПЛА (Sharifi et al., 2026). Еще одним самым распространяющим фактором нарушения безопасности может быть физический захват БПЛА из-за повышенной заметности БПЛА в воздушном пространстве (Yoo et al., 2025). Эти факторы дают злоумышленникам больше возможностей для взаимодействия с БПЛА для создания помех, подмены сигналов и перехвата данных нарушая связь управления и контроля, потенциально приводя к приостановке полета или непредсказуемому изменению траектории полета БПЛА.

В данном направлении множество исследований была посвящена классификации уязвимостей БПЛА, типам атак (Tang et al., 2025), включая разработки методов защиты (Romagnoli et al., 2023). При этом существующие подходы имеют разные точки зрения с учетом архитектуры системы БПЛА. Большинство из них демонстрируют основных векторов атак, направленные на полетный контроллер, наземную станцию управления и канал передачи данных, включая GPS-спуфинг, глушение сигналов, атаки типа DoS, подмену видеопотока и внедрение вредоносного кода. Множество работ за последние десятилетия были посвящены выявлению потенциальных слабых мест и классификации типов атак на основе уязвимостей архитектуры системы

БПЛА. В основном киберугрозы БПЛА классифицировались по целевым компонентам системы (полетный контроллер, наземная станция управления и канал передачи данных) и по возможностям злоумышленника (раскрытие данных, получение знаний о системе и нарушение работы) (Qiu et al., 2022). Множество уязвимых мест для атак со стороны злоумышленников в значительной степени связанны с беспроводными протоколами связи, бортовых датчиков и автоматизированными контурами управления (Yang et al., 2026).

Во многих исследованиях были рассмотрены современные виды атак на БПЛА и среди них самые распространённые виды были отмечены подмена GPS-сигнала, внедрение команд, подавление каналов передачи данных или отказ в обслуживании (DoS) (Tahavori et al., 2020). В последствии несвоевременного обнаружения и предотвращения атак на компоненты БПЛА могут привести к срыву миссий, нарушению конфиденциальности или даже нанесение физического вреда. При этом авторы (Zuev et al., 2018) отмечают о значительном повышении риска, в случаях, когда БПЛА работают автономно или взаимодействуют с наземными или облачными системами управления. В работе (Wang et al 2026), авторы утверждают, что атаки в виде глушения или подмены GPS-сигналов осуществляются для отключения системы навигации БПЛА. При этом на сегодняшний день GPS-сигналы в системах БПЛА часто не подлежат шифрованию, что существенно упрощает реализацию атаки и в последствии подмена сигнала ложными хаотичными координатами могут вызвать дезориентацию и падение БПЛА. Во многих случаях нарушение вещания позиций (аналог ADS-B) происходит из-за глушения сигналов управления GCS (Rezaee et al 2024). Нарушение связи приводит к активации режимов отказа, вызывая хаотичный полет БПЛА и может вызвать процесс столкновения, что приводит к аварийному исходу. Подмена сигналов в системе телеметрии и видеонаблюдения может ввести в заблуждение оператора, который управляет БПЛА дистанционно. Также существуют атаки в виде манипуляции захваченным видео. В данном случае перехват системных данных для замены реального видео на фальсифицированное позволяет злоумышленнику захватить контроль. Отмечается (Wang et al 2026) что данный способ атаки можно реализовать в комбинации с подменой GPS координат. Внедрение фальсифицированных данных с сенсоров БПЛА осуществляется с помощью внешнего вмешательства или внутренний доступ в целях дестабилизации режима полета. Злонамеренное аппаратные и вредоносные программные обеспечения (трояны, бэкдоры, командные инъекции и т.д.) могут быть внедрены для кражи конфиденциальных данных или же для намеренного отключения системы защиты чтобы вызвать сбой в системе управления БПЛА. Также отмечается важность своевременного предотвращения несанкционированного раскрытия коммуникаций системы БПЛА. Данный вид атак реализуется с целью несанкционированного получения и утечки персональных данных и может привести к компрометации

программного обеспечения диспетчеризации, формированию некорректных заданий, нарушению маршрутизации, операционным сбоям. Одним из наиболее распространённых типов атак на БПЛА считается атака типа «Отказ в обслуживании» (DoS). В большинство случаях незапланированная внезапная перегрузка вычислительных ресурсов или сетевых каналов БПЛА приводит к остановке операций, снижению производительности либо переводу системы в непредусмотренное состояние функционирования.

Общий анализ существующих исследований в данном направлении сводится к тому, что кибератаки на БПЛА могут охватывать все компоненты и подсистемы базовой архитектуры БПЛА и классифицируются следующим образом, представленной на рисунке 1.

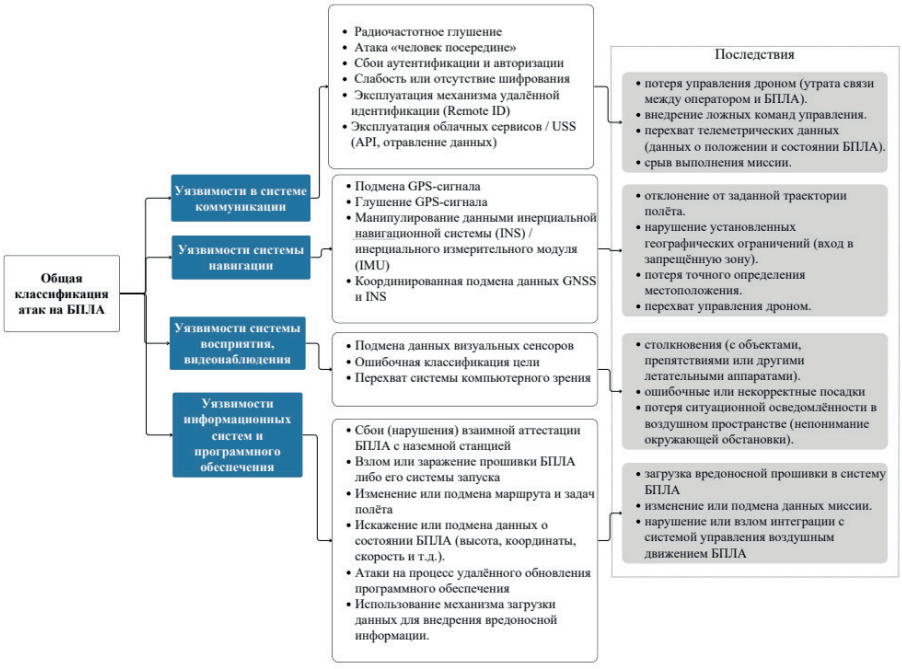

Рисунок 1 – Основная классификация существующих видов атак на базовую архитектуру БПЛА

За последние годы, рост использования БПЛА в значительной степени повышает их киберустойчивость. Отсутствие надёжной защиты делает их более уязвимыми для эксплуатации уязвимостей в программном обеспечении, внедрения вредоносных программ и несанкционированных модификаций программного обеспечения. Формирование надежной системы защиты и безопасность их компонентов становится необходимым для обеспечения его функциональности при выполнении в различных миссиях.

В данном направлении были проанализированы различные виды угроз безопасности на БПЛА. Демонстрируя всесторонний анализ существующих

атак исследователями (Qiu et al., 2022), была предложена модель киберугроз и были обсуждены методы повышения безопасности компонентов БПЛА. Также схожие работы были посвящены разработкам усовершенствованных методов шифрования канала связи, защиты от атак типа «отказ в обслуживании» (DoS) и систем обнаружения вторжений. В некоторых из них были получены интересные выводы. Одни авторы утверждают, если своевременное обнаружение пассивного перехвата и внедрение надежных протоколов шифрования и защищенных каналов связи может способствовать значительному повышению уровня безопасности БПЛА. Другая группа авторов в своих исследованиях (Yang et al., 2026) основное внимание уделили построению эффективного метода оценки состояния на основе полученных данных от систем интеллектуальных датчиков для обнаружения атак на данные связи БПЛА. Это позволило предотвратить перехвата конфиденциальной информации осуществляемые через навигационные команды, системы телеметрии. Также для защиты критически важных сведений об архитектуре и работе сети БПЛА и для обеспечения безопасной и надежной интеграции БПЛА в воздушное пространство многими регулирующими органами различных стран были разработаны руководящие принципы кибербезопасности. Изучая установленные нормативы кибербезопасности БПЛА, авторы (Tucker et al., 2026) пришли к тому, что в большей степени регламенты Federal Aviation Administration (FAA) предназначено для защиты каналов связи БПЛА от подмены, помех и несанкционированного доступа. В этом направлении аналогичный регламент European Union Aviation Safety Agency (EASA) описывает меры кибербезопасности и защиты данных для операций с БПЛА. Для защиты сетей беспилотных летательных аппаратов (БПЛА) от киберугроз криптографические методы, обеспечивающие конфиденциальность, целостность и аутентичность передаваемых данных, включая управление идентификацией на основе блокчейна. В дополнение к регламентам отмечается важность соответствия методом защиты к стандартам кибербезопасности ISO/IEC 27001.

На сегодняшний день были разработаны и проанализированы множество способов и методов, направленные на борьбу с атаками на БПЛА. Анализируя существующие передовые отраслевые практики формирования устойчивой системы кибербезопасности БПЛА применяются различные методы, которые классифицируются следующим образом, согласно таблице 1.

Таблица 1 – Классификация методов обнаружения кибератак в БПЛА

№	Метод обнаружения	Принцип работы	Примеры применения	Преимущества	Ограничения
1	Signature-Based	Сравнение трафика или поведения с известными шаблонами атак	IDS по правилам, проверка MAVLink-команд	Высокая точность для известных атак, низкая вычислительная нагрузка	Не выявляет новые (zero-day) атаки
2	Anomaly-Based	Обнаружение отклонений от нормального профиля работы	Анализ телеметрии, контроль задержек, частоты пакетов	Позволяет выявлять неизвестные атаки	Возможны ложные срабатывания
3	ML-Based	Классификация поведения на основе обученных моделей	Детекция GPS-спуфинга, DoS, инъекции телеметрии	Высокая адаптивность, выявление сложных атак	Требует обучающих данных и вычисл-ительных ресурсов
4	Cryptographic verification	Проверка целостности и аутентичности данных	Цифровые подписи, HMAC, secure boot	Высокая защита целостности и подлинности	Не выявляет поведенческие аномалии
5	Behavioral Detection	Сравнение фактического поведения с физической моделью полёта	Кросс-проверка GNSS и IMU, контроль траектории	Эффективен для навигационных атак	Требует точной модели движения

В сравнительном анализе современных методов обнаружения кибератак из Таблицы 1 были рассмотрены сигнатурные, аномальные, основанные на машинном обучении, криптографические и поведенческие методы обнаружения атак. Проведенный анализ показывает, что традиционные сигнатурные методы обеспечивают высокую точность обнаружения известных угроз, однако недостаточно эффективны против новых типов атак. В свою очередь, методы анализа аномалий и машинного обучения обладают более высокой адаптивностью и способны выявлять ранее неизвестные угрозы, но требуют значительных вычислительных ресурсов и качественных обучающих данных. Криптографические методы обеспечивают контроль целостности и подлинности данных, а поведенческий анализ позволяет выявлять навигационные атаки на основе сравнения фактических и ожидаемых параметров движения БПЛА.

Материалы и методы. Разностороннее изучение существующих

кибератак на БПЛА и эффективность применения существующих методов позволило разработать многоуровневую систему киберзащиты БПЛА, которая представлена на рисунке 2.

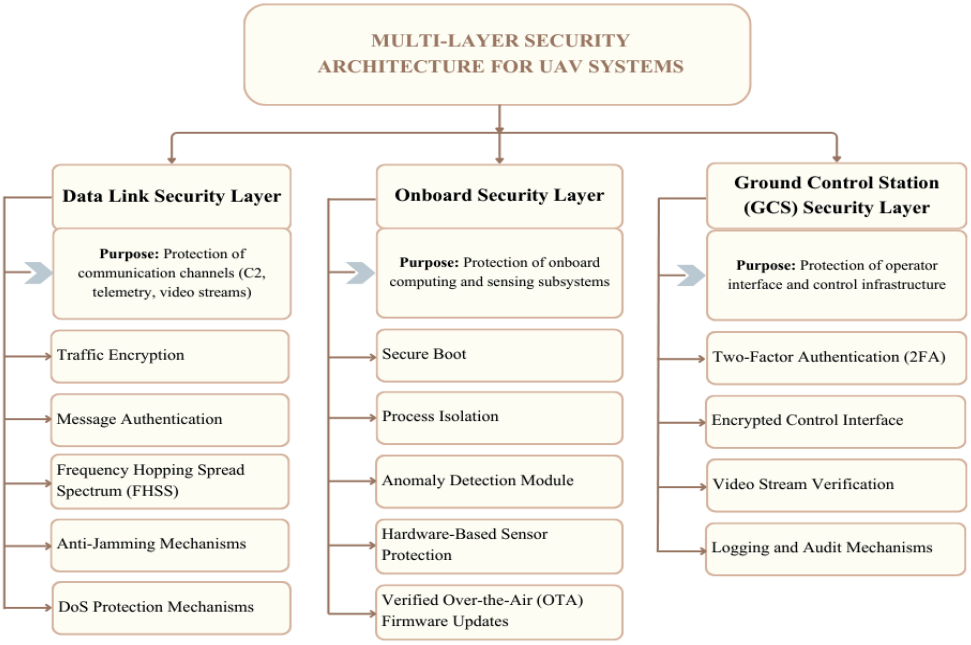

Рисунок 2 – Концептуальная архитектура системы киберзащиты БПЛА

В разработанной Концептуальной архитектуре системы киберзащиты БПЛА безопасность обеспечивается одновременно на уровне канала связи, бортовой вычислительной платформы и наземной станции управления. Представленный подход в отличие от существующих решений интегрирует защиту навигации, телеметрических потоков, сенсорного комплекса, исполнительных модулей и операторского интерфейса в единую непрерывную цепочку.

Для детализированного анализа эффективности предложенной многоуровневой архитектуры целесообразно рассмотреть её функциональные компоненты по отдельности. Среди них особое значение имеет телеметрический канал связи, поскольку именно он обеспечивает непрерывный обмен управляющими командами и параметрами полёта между бортовой системой и наземной станцией управления.

Телеметрический канал, обеспечивающий передачу управляющих команд и параметров полёта, является критическим компонентом БПЛА, уязвимым к инъекциям, подмене идентификаторов и нарушениям целостности пакетов. Структура телеметрической системы БПЛА представлена на рисунке 3.

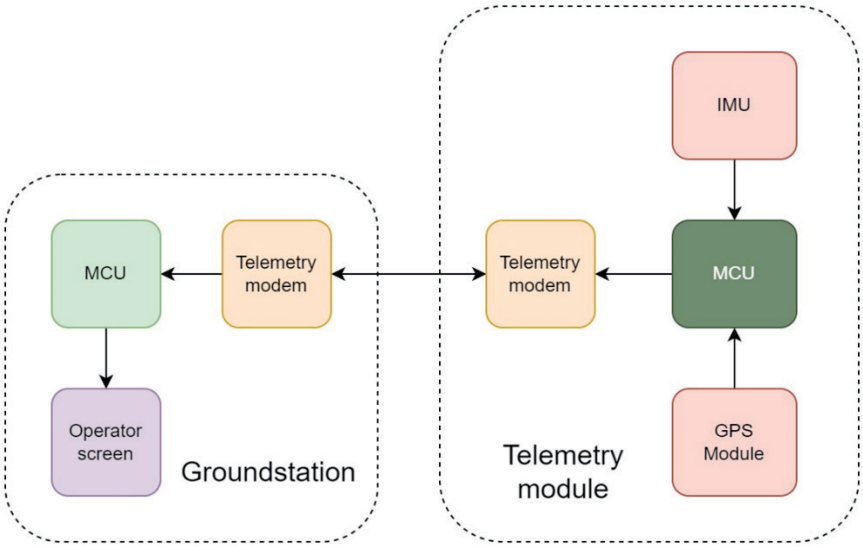

Рисунок 3 – Структура телеметрической системы БПЛА

На схеме представлена структурная организация телеметрического взаимодействия между наземной станцией управления и бортовым телеметрическим модулем БПЛА. Наземная станция включает микроконтроллер (MCU), операторский интерфейс и телеметрический модем, обеспечивающий двусторонний обмен данными. Управляющие команды от оператора передаются через MCU к радиомодему и далее по беспроводному каналу связи. Бортовой телеметрический модуль содержит собственный MCU, подключённый к навигационным и инерциальным датчикам (GPS Module, IMU). Телеметрический модем осуществляет приём управляющих команд и передачу параметров полёта (координаты, ориентация, скорость, состояние системы) обратно на наземную станцию. Анализ исследований выявил наиболее распространённых протоколов телеметрической связи, используемых БПЛА является MAVLink, User Datagram Protocol (UDP), Transmission Control Protocol (TCP) (Yu et al., 2025).

Протокол Micro Air Vehicle Link (MAVLink) в системах БПЛА применяется для обеспечения радиосвязи в пределах ограниченной зоны действия при средней скорости передачи данных в режиме прямой видимости (Dad et al., 2024). Особенностью MAVLink является низкая избыточность и малый размер пакетов, что делает его эффективным для радиоканалов с ограниченной пропускной способностью. Однако в базовой версии протокол не обеспечивает встроенного шифрования, что создаёт риски перехвата и инъекции сообщений. Протокола управления передачей TCP и UDP используется как транспортный протокол для передачи данных телеметрии в реальном времени. Они широкое применение нашли как в проводных, так и в беспроводных сетях. Применение TCP обеспечивает надежность,

гарантию доставки данных в определенном порядке и контроль перегрузки. Однако за счёт механизма подтверждений увеличивается время задержки, что ограничивает его применение в критичных к времени каналах управления. UDP в меньшей степени учитывает параметры надежности чем TCP, чтобы сосредоточиться на доставке пакетов данных в реальном времени. Это делает UDP предпочтительным для потоков телеметрии и видео, но одновременно повышает уязвимость к spoofing-атакам и packet injection (Yu et al., 2025).

На данном этапе исследования детальное изучение структуры сообщений, включая поля серийных номеров, логику проверки контрольной суммы и формальные определения полей данных предоставило возможность выявить три основных типа уязвимостей:

- отсутствие или слабость шифрования, замена пакетов;
- вызванная использованием предсказуемых идентификаторов;
-несогласованность в проверке контрольной суммы.

Эти результаты стали эмпирической основой для представления моделей угроз в телеметрическом модуле. Для более детального исследования была представлена структурно-функциональная схема программно-моделируемой системы анализа телеметрического обмена БПЛА.

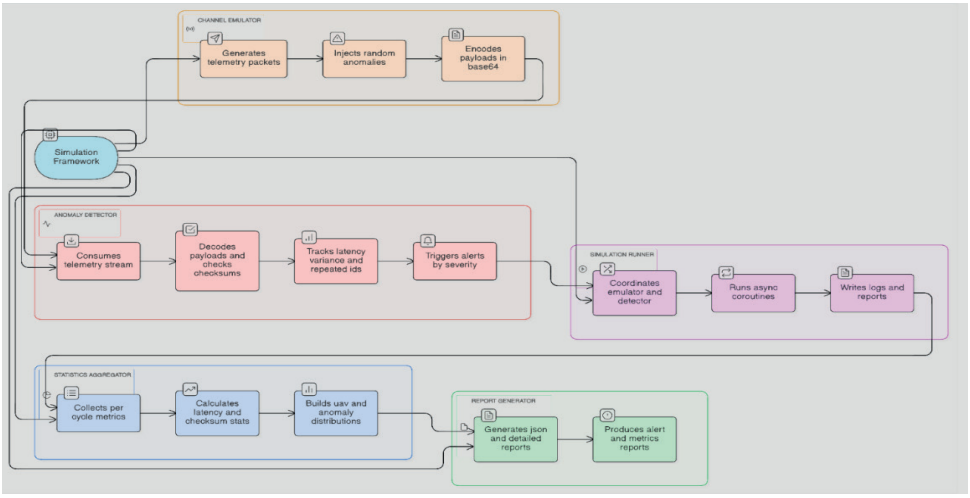

Рисунок 4 – Функциональная архитектура системы эмуляции и обнаружения аномалий телеметрического канала БПЛА

Функциональная архитектура системы эмуляции и обнаружения аномалий телеметрического канала БПЛА состоит из следующих модулей:

Для формирования телеметрических пакетов, инжектирования случайных аномалии и координации полезную нагрузку (base64) применяется Channel Emulator. Оно применяется для моделирования реальных условий передачи данных. Выполнение декодирования полезной нагрузки и проверку контрольных сумм применяется модуль Anomaly Detector. Оно осуществляет

анализ повторяющихся идентификаторов и вариаций задержки и инициирует оповещения в зависимости от уровня критичности. Сборка метрик по циклам обработки, вычисления статистики задержек и контрольных сумм, включая формирование распределения аномалий осуществляет модуль Statistics Aggregator. Координация взаимодействия существующих модулей осуществляется через Event Loop Runner. Report Generator формирует JSON-отчёты, журналы событий и сводные метрики системы.

В представленной функциональной архитектуре системы эмуляции и обнаружения аномалий телеметрического канала БПЛА механизм проверки контрольной суммы для пакетов MAVLink можно выразить следующим образом:

$$CRC_{valid} = \sum_{i=1}^{n} b_i \ mod\ 256 \quad (1)$$

где, CRC_{valid} – ожидаемое значение контрольной суммы, которая определяется вычислением из содержимого пакета MAVLink;

b_i – значение *i*-го байта в полезной нагрузке пакета телеметрии;

n – общее количество байт в полезной нагрузке пакета MAVLink;

mod 256 - операция модуля, гарантирующая, что контрольная сумма соответствует одному байту (0–255), которая соответствует структуре пакета MAVLink.

Для количественной оценки частоты нарушений в контрольной сумме коэффициент несоответствия определяется:

$$R_{CS} = \frac{N_{mismatch}}{N_{total}} \cdot 100\%, \quad (2)$$

где, $N_{mismatch}$ - количество пакетов, для которых вычисленная контрольная сумма не совпала с полученной контрольной суммой;

N_{total} – общее количество обработанных телеметрических пакетов в окне симуляции.

В условиях нормального режима функционирования типичное время доставки пакета от бортового модуля к наземной станции характеризуется средним значением задержки. Математическая модель задержек канала в данном случае определяется следующим образом:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} d_i \quad (3)$$

где d_i – задержка передачи i – го телеметрического пакета;

N – общее количество обработанных пакетов.

Индикатор нестабильности телеметрического обмена характеризуется дисперсией задержки, которая определяется:

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(d_i - \mu)^2 \quad (4)$$

Статистический критерий отклонения передачи пакетов от нормального режима оценивается критерием аномалий по задержке пакета и определяется следующим образом:

$$|d_i - \mu| > k\sigma \quad (5)$$

где k - порог чувствительности, обычно принимаются значения 2 (доверительный интервал ~95%) или 3 (доверительный интервал ~99.73%) и зависит от чувствительности детектора и вероятности возникновения ложных тревог;

Эффективность алгоритма детектирования характеризуется моделью оценки вероятности обнаружения атак:

$$P_D = \frac{N_{detected}}{N_{injected}} \quad (6)$$

где, $N_{detected}$ – количество искусственно внедрённых аномалий;

$N_{injected}$ - число корректно обнаруженных аномалий.

Вероятность правильного обнаружения атаки оценивается в пределах от 0 до 1.

$$0 \leq P_D \leq 1 \quad (7)$$

Вероятность ложного срабатывания определяется:

$$P_{FA} = \frac{N_{false}}{N_{normal}} \quad (8)$$

N_{normal} – число пакетов в нормальном режиме

N_{false} – число ошибочно классифицированных пакетов

Этот показатель оценивает вероятность того, что система объявляет аномалию при её отсутствии. Если значение чрезмерно высокий, то может привести к ненужным реакциям защиты и снижению доверия к системе.

Пороги для задержки, ошибок контрольной суммы и повторяющихся идентификаторов можно задать с применением параметров latency_threshold, checksum_threshold, repeat_id_threshold. Они позволяют более детально настраивать чувствительность обнаружения аномалий. В случае если пороги превышают установленную норму, то событие регистрируется в системе с следующих категориях уровней тяжести: средний, высокий и критический. Тогда оценка серьёзности угрозы в системе многоуровневой модели будет выглядеть следующим образом:

$$S_i = \begin{cases} critical & if\ R_{CS} > \theta_{CS}^{high}\ AND\ f_j > \theta_{id} \\ high & if\ R_{CS} > \theta_{CS}^{high}\ OR\ |d_i - \mu| > 3\sigma_d \\ medium & if\ payload_{malformed} = true\ OR |d_i - \mu| > 2\sigma_d \end{cases} \quad (9)$$

где S_i– классификация серьёзности, присваиваемая i-му обнаруженному аномалии;

θ_{CS}^{high} – параметр порога несоответствия верхней контрольной суммы (checksum_threshold);

f_j – частота повторения идентификатора БПЛА в текущем окне обработки определяется соотношением числа появлений идентификатора в общее число пакетов N:

$$f_j = \frac{n_j}{N} \quad (10)$$

θ_{id} – параметр порога повторения идентификатора (repeat_id_threshold);

$payload_{malformed}$ – булев индикатор, равный моменту, когда полезная нагрузка пакета, декодированная в Base64.

Для верификации предложенной архитектурной модели была выполнена её практическая реализация в среде Python 3.12, в рамках которой разработана программная платформа симуляции телеметрического канала БПЛА.

Реализация осуществляется на совместной работе модулей генерации телеметрических пакетов, механизм инъекции аномалий, включая подсистему детектирования нарушений и блоков статистической обработки результатов.

Результаты. Обработка телеметрии рассматривается как непрерывный процесс с постепенным накоплением статистики, что позволяет фиксировать даже слабовыраженные признаки попыток атаки. Предъявленные требования и технические спецификации к безопасности и киберзащите основаны на программных возможностях, которые необходимы соблюдать в системе БПЛА для обнаружения основных форм помех или повреждений. В частности, система должна уметь выявлять отсутствующие участки, ошибочно сгенерированные полезные нагрузки и поддельные идентификаторы БПЛА.

Характер атак реализуемые в телеметрическом канале нарушают целостность, подлинность или непрерывность функциональности БПЛА что является критически опасным.

Разработанная архитектура системы обеспечивает реализацию модульной программной платформы, которая должна имитировать реалистичную телеметрическую среду для БПЛА. Структура защиты основана на трёх функциональных уровнях: профилактика; обнаружение; реагирование. Каждый модуль концептуально отличался друг от друга, но был разработан для взаимодействия в общей моделирующей среде. В этом цикле отчётности акцент делался на уровне обнаружения, и планировалось более глубоко интегрировать уровни профилактики и реагирования на следующих этапах.

Уровень предотвращения обеспечит криптографическую защиту и защищённые протоколы передачи, однако с точки зрения управления ключами он сложнее, и его реализация рассматривается после завершения разработки механизмов обнаружения аномалий. Уровень отклика позволяет выдавать предупреждения и вызывать системные реакции на основе подтверждения наличия телеметрических аномалий. На данном этапе этот модуль разработан в базовом виде с наличием элементарных функций. Этот процесс будет реализован в зависимости от результатов тестирования и возможностей обнаружения атак в более сложных сценариях. Рабочий процесс сформирован визуальным образом и представлено на рисунке 5.

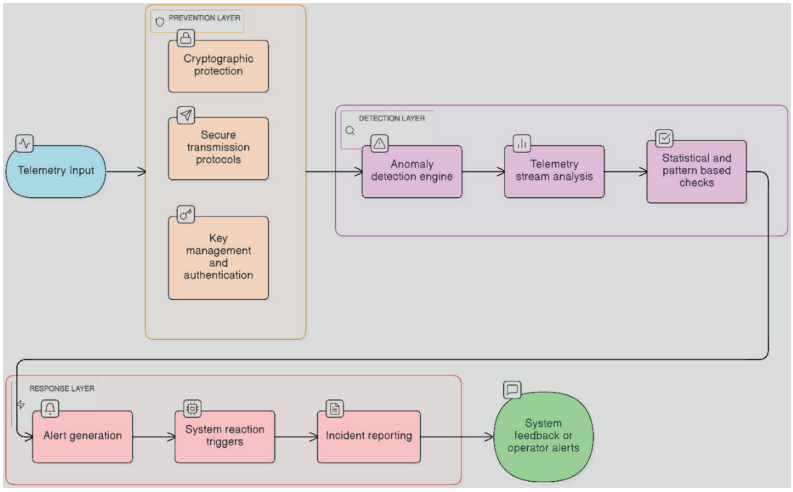

Рисунок 5 – Многоуровневая архитектура киберзащиты телеметрического канала БПЛА

Многоуровневая архитектура киберзащиты телеметрического канала БПЛА обеспечивает непрерывную цепочку защиты телеметрического обмена БПЛА.

Платформа симуляции в программной среде Python 3.12 состоит из выжных трех модулей ChannelEmulator, AnomalyDetector и SimulationRunner.

Эти модули разрабатывались в итерациях, каждый из которых независимо проходил модульное тестирование и верифицировался для обеспечения внутренней согласованности результатов и прослеживаемости.

Эмулятор канала является источником телеметрических данных. Он генерирует синтетические пакеты с реалистичными идентификаторами БПЛА, временными метками и другими параметрами полёта, такими как высота, скорость, курс и уровень заряда батареи. Зашифрованный канал связи и полезные нагрузки кодируются в блоке Base64. Система также обладает контролируемой инъекцией аномалий: случайно введённые ошибки включают потерю пакетов, искажённые полезные нагрузки и поддельные идентификаторы БПЛА. Это позволяет наблюдать эффективность системы в повторяемых, полуслучайных условиях.

Другой важный компонент, AnomalyDetector, обеспечивает функциональность основного анализа. Он потребляет поток телеметрии в реальном времени, декодирует каждую полезную нагрузку и проверяет встроенные контрольные суммы. Также он рассчитывает и отслеживает статистические показатели, такие как дисперсия задержки и повторяющиеся идентификаторы БПЛА, чтобы выявлять необычные закономерности.

Пороги для задержки, ошибок контрольной суммы и повторяющихся идентификаторов можно задать с помощью параметров: latency_threshold, checksum_threshold, repeat_id_threshold. Они позволяют тонко калибровать чувствительность обнаружения. Если эти пороги превышаются, событие регистрируется системой с назначенным уровнем тяжести: средний, высокий или критический.

SimulationRunner связывает оба компонента вместе, управляя процессом выполнения. Он гарантирует, что ChannelEmulator и AnomalyDetector работают одновременно с использованием asyncio корутинов Python, эмулируя реальный канал связи в реальном времени. Взаимосвязь представленных модулей и компонентов отображена на рисунке 6.

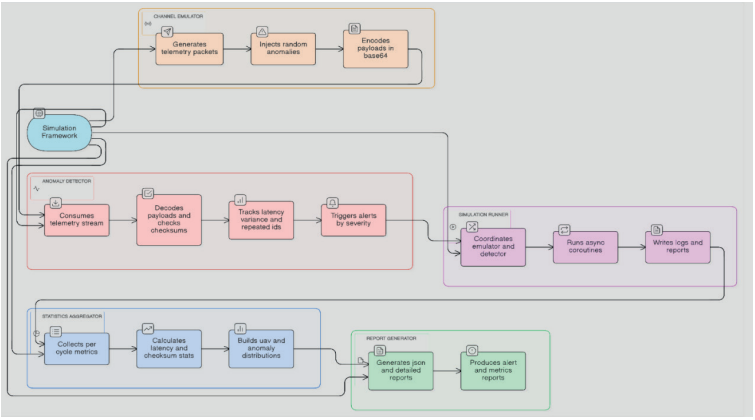

Рисунок 6 – Взаимосвязь модулей и компонентов

Детерминированные случайные начальные значения используются для обеспечения повторяемых результатов очень важной особенностью для верификации и регрессионного тестирования. После каждого прогона SimulationRunner выдает два вида выходных данных: файл .log с меткой времени, записывающий все обнаруженные аномалии, и структурированный отчет .json, обобщающий ключевые метрики из выполнения, тем не менее, как заключение записанных модулей и компонентов, следующая диаграмма объясняет взаимосвязь между компонентами, которые были закодированы.

Обсуждение. Для проверки работоспособности архитектуры была проведена серия экспериментов в разработанной среде симуляции. Основные результаты работы симуляционной платформы телеметрического канала БПЛА представлены на таблице 2.

Таблица 2 – Основные результаты работы симуляционной платформы телеметрического канала БПЛА

№	Показатель	Значение	Интерпретация
1	Количество циклов симуляции	100	Представительный прогон модели
2	Доля инъекции аномалий	10%	Контролируемая нагрузка на систему детекции
3	Обработано пакетов	97	Незначительные потери, обусловленные моделируемыми сбоями
4	Обнаружено несовпадений контрольных сумм	6	Выявлены нарушения целостности данных
5	Общее число зафиксированных аномалий	118	Система демонстрирует высокую чувствительность
6	Средняя задержка пакета	0.037 сек	Стабильная работа канала при нагрузке
7	Дисперсия задержки	1.45×10^{-4}	Низкая вариативность передачи
8	Форматы выходных данных	.log, .json	Двойная верификация и трассируемость
9	Повторяемость эксперимента	Deterministic random seeds	Обеспечение воспроизводимости результатов
10	Среда реализации	Python 3.12 (asyncio)	Асинхронная обработка телеметрии

Большинство событий в полученных результатах симуляций классифицировано как значимые и распределение по уровню критичности составило 100 high, 14 medium, 4 critical.

С точки зрения обработанных данных, большинство аномалий были вызваны высокими показателями отказа контрольной суммы, необычно частыми повторениями идентификаторов БПЛА или идентификацией поддельных меток БПЛА, таких как UAV_612, UAV_162 и UAV_678. Все обнаруженные аномалии регистрировались в файле с названием

anomalies_20251112_163329.log. Журнал событий этого .log файла представлена на рисунке 7.

Рисунок 7 – Log view

Соответствующий отчет .json содержит общее количество обработанных пакетов, статистику задержек и сведения о серьезности, а также временные метки выполнения, которые дают количественное представление каждого прогона моделирования. Структура регистрации, разработанная на этом этапе, оказалась очень полезной для устранения неполадок и проверки достоверности данных. Фактически, неожиданное поведение, такое как отложенные оповещения или пропуски записей об аномалиях, было гораздо проще диагностировать путем сравнения выходных данных в форматах .log и .json. Поддержание этой системы с двойным выходом гарантирует, что каждая аномалия будет хронологически задокументирована и аналитически обобщена, как показано на следующем рисунке 8.

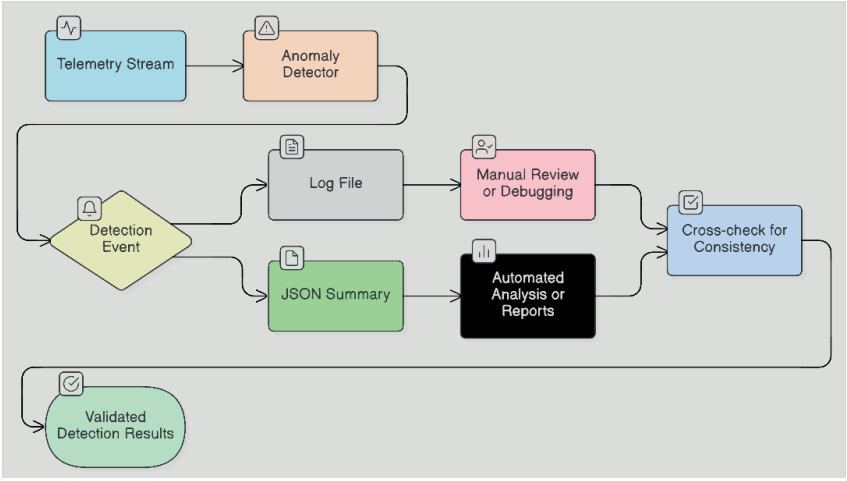

Рисунок 8 – Механизм двойного выхода

Если статистический телеметрический анализ будет постоянно применяться и поддерживаться модульными инструментами моделирования

то в дальнейшем оно имеет возможность предоставить практическую основу для раннего обнаружения аномалий даже при отсутствии алгоритмов машинного обучения. Этот вклад является важным шагом к созданию полноценной системы киберзащиты для платформ БПЛА.

Выводы. Результаты проведённых симуляционных экспериментов раскрывают характер реакций бортовой системы в условиях навигационных и телеметрических искажений, формируемых в контролируемой среде моделирования. Симуляция и тестирование проводилось в последовательном порядке наблюдения за системой, работающей в режиме непрерывной передачи данных. Оно не просто дает возможность фиксировать факт нарушения нормальной работы, но и может анализировать траекторию возникновения аномалий, их развитие и момент перехода системы из устойчивого состояния в предаварийное или аварийное.

Практическая реализация архитектуры в виде программной симуляционной платформы в среде Python 3.12 обеспечила воспроизводимое моделирование телеметрического обмена и контролируемую инъекцию аномалий. Результаты серии экспериментов подтвердили эффективность статистического метода обнаружения аномалий на основе анализа задержек, повторяемости идентификаторов и ошибок контрольных сумм. Система продемонстрировала устойчивость к моделируемым воздействиям при сохранении стабильных временных характеристик передачи данных. Детерминированный статистический анализ телеметрических потоков способен обеспечить раннее выявление киберугроз без привлечения ресурсоёмких алгоритмов машинного обучения, что особенно важно для систем с ограниченными вычислительными ресурсами.

Перспективы дальнейших исследований связаны с углублённой интеграцией криптографического уровня защиты, расширением сценариев атак, а также тестированием предложенного подхода в аппаратно-реальных условиях функционирования БПЛА.

References

Alshamrani A., and Alghamdi A.M. (2026) Zero-Shot Attack Detection in UAV Networks Using Foundation Models. Alexandria Engineering Journal, 136. – P. 105–124. https://doi.org/10.1016/j.aej.2025.12.065 (in Eng.).

Alsumayt A., Nagy N., Alsharyofi S., Alahmadi R., Al-Rabie R., Alesse R., Alibrahim N., Alahmadi A., Alghamedy F. H., and Alfawaer Z. (2026) Cutting-Edge DoS Attack Detection in Drone Networks: Leveraging Machine Learning for Robust Security. Sci, 8(1). – P. 20. https://doi.org/10.3390/sci8010020 (in Eng.).

Burbank J., Caleb T., Andam E., and Kaabouch N. (2026) Detection and Mitigation of Cyber Attacks on UAV Networks. Electronics, 15(2). – P. 317. https://doi.org/10.3390/electronics15020317 (in Eng.).

Islam M. S., Mahmoud A. S., and Sheltami T. R. (2025) AI-Enhanced Intrusion Detection for UAV Systems: A Taxonomy and Comparative Review. Drones, 9(10). – P. 682. https://doi.org/10.3390/drones9100682 (in Eng.).

Mohammed U. M., Omolara A. E., Abiodun O. I., Rasheed J., Osman O., Lar P. M., Adeyinka P.

O., and Olugbenga A. G. (2025) Cyber Threat in Drone Systems: Bridging Real-Time Security, Legal Admissibility, and Digital Forensic Solution Readiness. Frontiers in Communication and Networks, 6. – P. 1661928. https://doi.org/10.3389/frcmn.2025.1661928 (in Eng.).

Qiu S., and Liu H. (2022) A New Zonotope-Based Attack Detection Method for UAV. 2022 41st Chinese Control Conference (CCC), Hefei, China. – P. 4276–4280. https://doi.org/10.23919/CCC55666.2022.9902124 (in Eng.).

Rezaee H., Salvato E., Fenu G., and Parisini T. (2024) Resilient Coverage by Teams of Quadrotor UAVs: Theory and Experiments. IEEE Transactions on Control Systems Technology, 32(6). – P. 2009–2022. https://doi.org/10.1109/TCST.2024.3389350 (in Eng.).

Romagnoli R., Krogh B. H., de Niz D., Hristozov A. D., and Sinopoli B. (2023) Software Rejuvenation for Safe Operation of Cyber–Physical Systems in the Presence of Run-Time Cyberattacks. IEEE Transactions on Control Systems Technology, 31(4). – P. 1565–1580. https://doi.org/10.1109/TCST.2023.3236470 (in Eng.).

Sharifi I., Ghazanfari M., Taye A., Wei P., Ahmed M. H., Kim H. T., Ghasemi M., Gupta V., Dahle N., Canady R., Diaz Gonzalez A., Coursey A., Bjorkman B., Lemieux-Mack C., Ward B. C., Koutsoukos X., Biswas G., Herencia-Zapana H., Hasan S., Amundson I., Fotiadis F., Topcu U., Lu J., Chen Q. A., Aryal N., Ibrahim A., Ras A. K., and Shirkhodaie A. (2026) A Survey of Security Challenges and Solutions for UAS Traffic Management (UTM) and Small Unmanned Aerial Systems (sUAS). arXiv. – P. 2601.08229. https://arxiv.org/abs/2601.08229 (in Eng.).

Tahavori M. (2020) A System-Theoretic Measure for Quantification of Vulnerabilities to Cyber Attacks with Application to Unmanned Aerial Vehicles. 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT), Prague, Czech Republic. – P. 492–495. https://doi.org/10.1109/CoDIT49905.2020.9263905 (in Eng.).

Tang H., and Chen Y. (2025) Composite Observer-Based Resilient MPC for Heterogeneous UAV-UGV Systems Under Hybrid Cyberattacks. IEEE Transactions on Aerospace and Electronic Systems, 61(4). – P. 8277–8290. https://doi.org/10.1109/TAES.2025.3542737 (in Eng.).

Tlili F., Ayed S., and Fourati L. C. (2024) Exhaustive Distributed Intrusion Detection System for UAVs Attacks Detection and Security Enforcement (E-DIDS). Computers & Security, 142. – P. 103878. https://doi.org/10.1016/j.cose.2024.103878 (in Eng.).

Tucker R. S., Nadeem M., and Pervez S. (2025) Real-Time Detection and Mitigation of GPS Spoofing in UAV Systems. 2025 12th International Conference on Information Technology (ICIT), Amman, Jordan. – P. 154–160. https://doi.org/10.1109/ICIT64950.2025.11049153 (in Eng.).

Wang P., et al. (2026) QUADFormer: Learning-Based Detection of Cyber Attacks in Quadrotor UAVs. IEEE Transactions on Control Systems Technology, 34(1). – P. 59–73. https://doi.org/10.1109/TCST.2025.3598255 (in Eng.).

Yang H., Yu Z., and Zhang Y. (2026) Observer-Based Adaptive Resilient Fault-Tolerant Cooperative Control for Multiple Fixed-Wing UAVs Subject to Cyberattacks and Actuator Faults. IEEE Internet of Things Journal, 13(3). – P. 5179–5192. https://doi.org/10.1109/JIOT.2025.3642912 (in Eng.).

Yoo J. D., Kim G. M., Song M. G., and Kim H. K. (2025) MeNU: Memorizing Normality for UAV Anomaly Detection with a Few Sensor Values. Computers & Security, 150. – P. 104248. https://doi.org/10.1016/j.cose.2024.104248 (in Eng.).

Yu A., Kolotylo I., Hashim H. A., and Eltoukhy A. E. E. (2025) Electronic Warfare Cyberattacks, Countermeasures, and Modern Defensive Strategies of UAV Avionics: A Survey. IEEE Access, 13. – P. 68660–68681. https://doi.org/10.1109/ACCESS.2025.3561068 (in Eng.).

Zuev A., Gryb O., Shvets S., and Makarov V. (2018) Evaluating and Ensuring the Cybersecurity of Power Line Remote Monitoring Systems. 2018 IEEE 3rd International Conference on Intelligent Energy and Power Systems (IEPS), Kharkiv, Ukraine. – P. 271–274. https://doi.org/10.1109/IEPS.2018.8559572 (in Eng.).

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Requirements for articles design for publication in the journal are available on the websites:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Managing Editor: *A.Shormakova*
Editors: *D.S. Alenov, T. Apendiev*
Computer layout: *G.D. Zhadyranova*

Signed for print: June 15, 2026
Format: 70×90 1/16. 26.5 printed sheets. Order No. 2.

«Central Asian Academic Research Center» LLP
Almaty, Shevchenko Street, 28