DOI10.58880/DKU.2026.02.02

МРНТИ 81.93.29, 73.31.17

УДК 629.7.05:004.056

КИБЕРБЕЗОПАСНОСТЬ АВИАЦИОННЫХ СИСТЕМ И ПЕРСПЕКТИВЫ ЗАЩИТЫ

Д.Н. Батырбеков

Казахстанско-Немецкий университет

Казахстан, г. Алматы

Аннотация

В статье осуществлен анализ основ кибербезопасности авиационных систем, прогнозируются основные вызовы и задачи для отрасли. В статье выявлено, что кибербезопасность авиационных систем – это сложная и многогранная сфера, которая охватывает как бортовую авионику воздушного судна, так и наземную инфраструктуру аэропортов, центры управления воздушным движением и информационные сервисы авиакомпаний.

Ключевые слова: кибербезопасность авиационных систем, киберриски, цифровые бортовые системы.

Введение

Цифровизация гражданской авиации быстро развивается: самолёты сегодня – это сложные информационно-связные комплексы, связанные между собой и наземной инфраструктурой через радиосети, спутники и интернет. Повышение уровня «связности» самолётов и сопутствующих систем открывает новые возможности для оптимизации полётов, но одновременно создаёт новые риски информационной безопасности. Как отмечают эксперты, кибератаки могут вызвать отказы авионики и привести к авиационным инцидентам. Хотя на сегодня не было публично подтверждённых случаев, когда именно хакеры стали причиной аварии, но уже произошли ситуации, когда сбои в цифровых системах самолётов близки к катастрофе. Например, при аварии Boeing 747-244SF авиакомпании MK Airlines в 2004 году ошибки в ПО бортовых компьютеров привели к падению самолёта при взлёте [1]. Анализ таких инцидентов показывает уязвимость интегрированных систем и подчёркивает необходимость защиты от умышленных воздействий.

Международные организации давно признают эту проблему. В руководстве ИКАО (Международная организация гражданской авиации) по расследованию авиационных происшествий уже упоминаются цифровые системы и указывается необходимость их защиты. В декабре 2024 года на Генеральной ассамблее ООН по гражданской авиации представители 31 страны одобрили декларацию, призывающую придавать вопросам авиационной безопасности и кибербезопасности равный приоритет [2], [3]. Данная декларация подчёркивает важность обмена информацией о киберугрозах, подготовки

квалифицированных кадров и реализации стратегии ИКАО по кибербезопасности гражданской авиации [4]. Таким образом, кибербезопасность сегодня входит в число основных задач мирового авиационного сообщества.

Поэтому исследование данных угроз и методов защиты авиационных систем становится всё более актуальным. Введение стандартов сертификации ПО (DO-178C), системного проектирования с учётом ИБ (DO-326A/ED-202A) и требований регуляторов (EASA, FAA) уже начали учитывать риски несанкционированного вмешательства. Однако в реальности, авиакомпании нередко сталкиваются с реализацией этих рисков – например, в 2024 году атака на систему электронного обслуживания пассажиров Collins Aerospace MUSE парализовала регистрацию в нескольких аэропортах Европы [5]. В этой статье мы рассмотрим современные цифровые системы самолётов и их уязвимости, опишем известные киберинциденты в авиации, а также существующие и перспективные меры защиты от таких угроз.

Современные цифровые системы и риски

Современный пассажирский самолёт содержит множество взаимосвязанных цифровых систем: от пилотажно-навигационных компьютеров до развлекательных сетей на борту. Ключевыми подсистемами являются системы управления полётом (FMS – Flight Management System), автопилота и бортовых вычислительных сетей (ARINC 429/664), системы навигации (GPS, инерциальные датчики, радиоориентирамент), средства связи (ACARS, VHF/UHF радио, спутниковые модемы) и различные датчики (TCAS, RADAR, ADS-B). Рисунок ниже иллюстрирует типичную архитектуру авионики современного самолёта (структура электроники внутри фюзеляжа и крыльев):

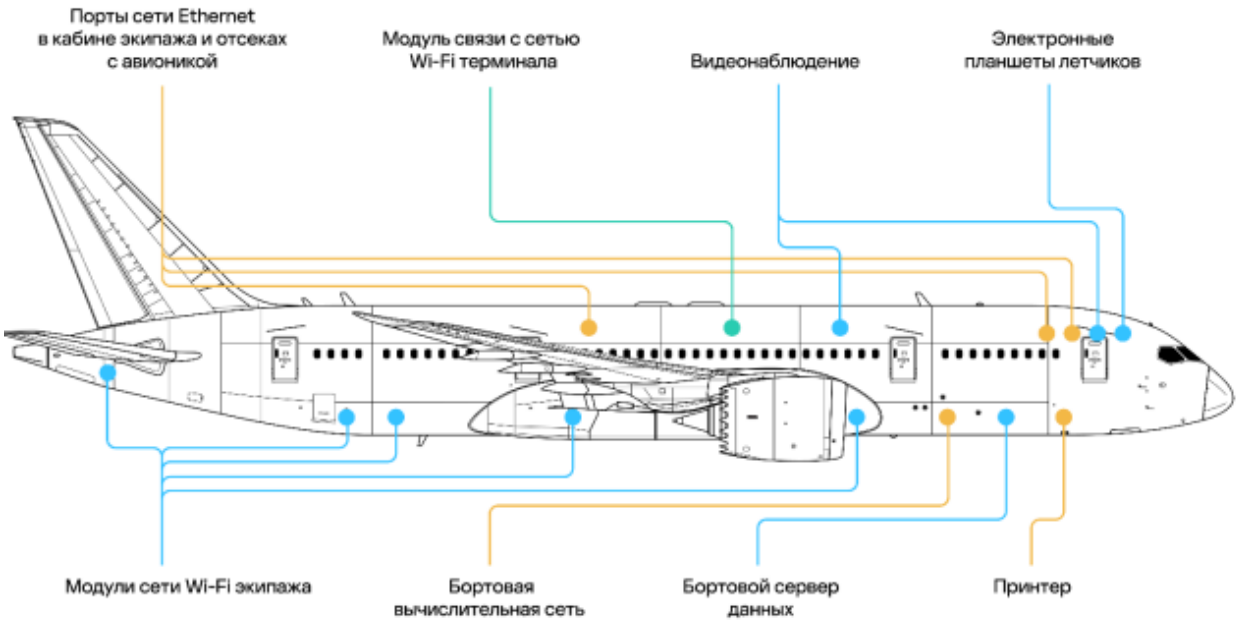

Рисунок 1 - Цифровые бортовые системы самолета Boeing 787 Dreamliner [6].

На рисунке хорошо видны основные цифровые бортовые системы. Для полёта самолёт использует одновременно несколько источников информации: спутниковую навигацию (GPS), наземные радиомаяки. Сообщения экипажа и диспетчеров передаются через цифровые каналы ACARS (Aircraft Communications Addressing and Reporting System) и радиосвязь. С учётом всего этого потенциал кибер-нападения велик:

- Системы навигации и позиционирования. GPS сигнал легко подделать (спуфинг) или заглушить. Такие инциденты уже случались: например, в январе 2025 года рейс Ryanair был вынужден отклониться от посадки в Вильнюсе из-за массовых помех GPS-сигналу в этом регионах [7]. Современные самолёты используют резервные инерциальные системы и вспомогательные радионавигационные источники, но прямой урон безопасности при зависании GPS очевиден – пилоты вынуждены переходить на альтернативные системы, что усложняет посадку и вводит задержки [8]. ADS-B (автоматическая зависимая слежка) – спутниково-раскрывное оповещение о положении самолёта – полностью открытая технология без аутентификации. Её можно заглушить или создать ложные цели, нарушив контроль за трафиком (такие исследования показали уязвимость ADS-B) [9].

- Бортовая связь (ACARS, CPDLC, радио). ACARS обеспечивает передачу текстовых сообщений между самолётом и наземными службами. Многие каналы ACARS и CPDLC реализованы без шифрования или слабо защищены. Исследования показывают, что перехват/подмена таких сообщений может вмешиваться в планирование полёта и даже управление экипажем [10]. В 2018 году исследователь Рубен Сантамарта продемонстрировал, что уязвимости спутниковых терминалов на борту (приводящие к управлению каналом FANS/CPDLC/ACARS) могут быть использованы для воздействия на эти системы [11]. Атаки на наземные ретрансляторы ACARS позволяют проникнуть в сеть авиакомпании.

- Бортовые сети и компьютеры. В современных самолётах всё больше функций интегрируется в «модульную авионику» (IMA – Integrated Modular Avionics). Одним из средств обеспечения разделения задач в IMA является стандарт ARINC 653, который задаёт пространственно-временные разделы (partitioning) для приложений разного уровня критичности. Это помогает изолировать отказ критического модуля от других, но не защищает от уязвимостей самого ПО. К примеру, программные ошибки в приложениях центрального компьютера Boeing 787 в 2020 году привели к отказам, а исправления появлялись долго [12]. Помехи или вредоносный код в ФМС могут вызвать некорректный расчёт траектории или управления, что опасно при взлёте/посадке. Кроме того, на борту часто работают электронные планшеты (EFB – электронный полётный планшет), соединённые с бортовой сетью. Была выявлена уязвимость в приложении Flysmart+ на iPad, когда специалисты Касперского обнаружили возможность вмешательства в процесс полёта через ПО EFB [13]. Даже пассажирская Wi-Fi-сеть теоретически может стать точкой входа: несмотря на то, что она обычно отделена от систем управления, исследования Сантамарты показали, что через бортовую Wi-Fi и уязвимости спутниковых терминалов можно получить доступ к внутренним подсистемам самолёта [14].

- Доступы с земли и аэропортов. На земле самолёт подключается к системам технического обслуживания, может загружать обновления ПО и навигационные данные. Если эти каналы незашифрованные, злоумышленник может внедрить фальшивые данные. Также возможна атака на авиасистемы аэропортов или

авиакомпаний (системы планирования, регистрации билетов и т. д.): прямые кибератаки на ИТ-инфраструктуру авиакомпании способны нарушить расписание и работу рейсов. Как показал опыт лета 2025 г.: мощная атака хакеров на информационные системы «Аэрофлота» привела к отмене примерно 42% рейсов в течение суток, тысячам ошеломлённых пассажиров и убыткам десятки миллионов долларов [15].

Для наглядности в Таблице 1 приведены основные категории угроз и примерные системы, на которые они могут повлиять/

Таблица 1 - Примеры киберугроз и их влияния на бортовые и наземные системы самолёта.

Угроза	Затрагиваемые системы	Возможные последствия	Рекомендуемые меры противодействия
Заглушение/спуфинг GPS	Навигация (GPS, FMS), автопилот	Потеря навигационного сигнала, отклонение курса, аварийная посадка	Резервирование инерциальных систем, мониторинг целостности сигнала, использование альтернативных радионавигационных средств

Угроза	Затрагиваемые системы	Возможные последствия	Рекомендуемые меры противодействия
Подмена ADS-B или радиомаяков	Системы слежения за трафиком (экипаж, АТС)	Ложные данные о положении самолётов, сбой диспетчерской обстановки	Внедрение криптографической аутентификации ADS-B, мультисенсорная верификация данных
Перехват/внедрение в ACARS	Связь экипажа с наземными службами (ACARS, CPDLC)	Ошибочные или ложные сообщения диспетчерам, сбой планирования полёта	Шифрование каналов, использование защищённых протоколов (IPSec), строгая аутентификация сообщений
Атака через Wi-Fi или спутниковую связь	Информационно-развлекательные и бортовые сети	Утечка данных, проникновение в подсистемы бортовых контроллеров	Сегментация сетей, межсетевое экранирование, регулярные проверки безопасности спутниковых терминалов

Зловредное ПО в авионике	Бортовые компьютеры (пилотаж, FMS, ARINC)	Сбой работы автопилота, некорректное управление, отказ критических систем	Строгий контроль целостности ПО, цифровая подпись обновлений, применение DO-178C и DO-326A

Таким образом, наиболее уязвимы именно сетевые и беспроводные компоненты авиационной системы, поскольку они открыты для внешнего доступа. В то же время сами авиационные сети (ARINC 429/664, AFDX) проектировались преимущественно с прицелом на надёжность и предсказуемость работы, но не на криптографическую защиту. Это приводит к тому, что многие угрозы остаются на уровне «низкой сложности» для реализации злоумышленниками.

Реальные случаи кибератак в авиации

На сегодняшний день не произошло ни одной публично признанной кибератаки, которая непосредственно привела бы к катастрофе самолёта. Тем не менее ряд инцидентов показывает, что атаки в авиационной сфере уже становятся реальностью и способны вызвать серьёзные сбои в работе перевозчиков и аэропортов.

- 2015: инцидент с исследователем на борту самолёта. В апреле 2015 года ИТ-специалиста Криса Робертса задержали после того, как он на борту рейса United Airlines написал в Twitter, что может «взять управление кислородными масками» самолёта. Сотрудники безопасности сняли его с рейса, а ФБР допросило исследователя. По словам Робертса, он ещё ранее тестировал системы самолётов: он якобы через встроенный Wi-Fi имел доступ к бортовым компьютерам, что позволило ему «вывести самолёт из заданного эшелона» [16]. Сам Робертс утверждал, что ряд его действий были преувеличены, но инцидент продемонстрировал, насколько серьёзно компании относятся к угрозам информационной безопасности. Сам авиаперевозчик в заявлении подчеркнул, что «считает свое управление полётом неспособным к несанкционированному доступу теми методами, которые описал Робертс» [17], однако инцидент ещё раз обратил внимание общественности на потенциальные уязвимости встроенных бортовых сетей.

- 2017: удалённый взлом Boeing 757. На международной конференции 2017 года агент Министерства внутренней безопасности США (DHS) объявил, что группа экспертов смогла снаружи взломать стоящий на земле Boeing 757 через радиоканал [18]. Хотя подробностей не раскрыли, этот факт подтверждает, что современные самолёты можно скомпрометировать даже в безопасном режиме через сбытые радиоуправляемые каналы. Последствия могли быть опасными: потеря жизненно важных функций самолёта в зоне аэропорта может привести к катастрофе. Этот случай подчёркивает, что кибервзломы самолётов перестают быть лишь теоретическим сценарием.

- 2018: демонстрация взлома спутниковой связи. Исследователь Рубен Сантамарта в 2018 г. на конференции Black Hat продемонстрировал реальную атаку на бортовой Wi-Fi и спутниковые терминалы самолётов [19]. Удалённо с земли ему удалось проникнуть в сеть авиапассажиров и получить контроль над SATCOM-модемом. Более того, он показал, что при помощи уязвимостей спутникового оборудования

можно «оружейно» воздействовать на самолёт – например, нарушать управление каналами связи ACARS/CPDLC [20]. Хотя атака выполнялась на «стенде», а не в полёте, Сантамарта отметил, что это уже не сценарий фантастики: «Это реальные случаи. Они больше не теоретические» [21]. Он обнаружил сотни самолётов, чья связь открыта в интернете, и доказал, что уязвимости в Satcom позволяют «использовать эти устройства в качестве оружия» [22].

- 2024: атака на систему регистрации пассажиров. 19 сентября 2024 г. произошёл крупный инцидент с кибератакой на Collins Aerospace – производителя систем обслуживания пассажиров (MUSE), используемых в аэропортах. В результате сбой в его программном обеспечении парализовал киоски регистрации и сдачи багажа в Брюсселе, Берлине (Бранденбург) и Лондоне (Хитроу) [23][24]. Из-за этого около 9 рейсов были отменены, десятки задержаны, а пассажиры вынуждены были регистрироваться вручную [25]. По словам экспертов, вредоносный код, по-видимому, заразил систему Collins; позднее агентство ENISA подтвердило, что это был рейнсомвер (шифровальщик) [26]. Сам производитель заявлял, что «исправляет проблему» и что последствия ограничены системой проверки билетов и багажа [27], но масштаб инцидента показал, как атака на узловой поставщик (систему, объединяющую несколько авиакомпаний) может расползтись по всей Европе. Специалисты подчёркивали, что «сектор авиации вложил много в безопасность полётов, но киберстойкость отстаёт» [28]. В статье Forbes отмечено, что в результате сбоя системы «Аэрофлота» на 28 июля 2025 г. были отменены 42% рейсов компании (около 110 из 260 запланированных), пострадали более 20 000 пассажиров, а ущерб оценили в десятки миллионов долларов [29]. Российские правоохранители уже возбудили уголовное дело по факту «неправомерного доступа к информационной системе» авиакомпании [30]. Как заявили сами хакеры («Silent Crow» и белорусские «Киберпартизаны BY»), они годами имели доступ к внутренней ИТ-инфраструктуре «Аэрофлота» и получили данные о полётах, базы CRM и переговоры персонала [31]. Этот случай демонстрирует, что атака на авиакомпанию в целом может настолько же эффективно заблокировать полёты, как и атака на самолёт.

Таким образом, реальные и демонстрационные случаи показывают широкий спектр угроз: от экспериментов внутри кабин до масштабных кибероперациий против авиакомпаний и аэропортов. Результатом всегда оказывается нарушение расписания полётов, отмены и задержки, а в долгосрочной перспективе – потеря доверия пассажиров и экономические убытки. Противостояние таким атакам требует как технических средств защиты на борту самолётов, так и усиления контроля над наземной инфраструктурой и цепочками поставок программного обеспечения.

Меры обеспечения кибербезопасности

Для защиты авиасистем используются как «традиционные» стандарты безопасности полёта, так и специально разработанные нормы информационной безопасности. Рассмотрим основные из них:

- ARINC 653 (разбиение на партиции). Этот промышленный стандарт задаёт правила пространственно-временного разделения (partitioning) приложений в авиационной системе. Каждое приложение («партиция») изолируется: оно получает собственную область памяти и выделенный временной срез процессора. ARINC 653 позволяет «на одном компьютере» запускать ПО разной критичности без их взаимного

вмешательства. Таким образом, неисправность либо вредоносный код в одном разделе не затрагивает работу других. Например, при внедрении непроверенных обновлений в ПО одного отделения грузоперевозок, разделение ARINC 653 не даст заразить код автопилота. Конечно, ARINC 653 само по себе не шифрует данные и не защищает от внешнего доступа, но оно повышает отказоустойчивость и сдерживает распространение вредоносных действий внутри бортовой сети.

- DO-178C (сертификация ПО). Это главный стандарт разработки программного обеспечения для авиации, признанный FAA/EASA/Transport Canada [33]. DO-178C задаёт процессы валидации, верификации и требований к документации ПО в зависимости от уровня его критичности (DAL, определяющий степень контроля за ошибками). Хотя сам по себе DO-178C сосредоточен на ошибках безопасности (safety), а не на защите от злоумышленников, строгие методы разработки снижают вероятность наличия «задних дверей» и делают приложения более надёжными. Уровни качества DO-178C (A–E) регламентируют тестирование и анализ кода: для самых критичных систем автопилота или управления полётом требуется полная прослеживаемость требований, 100% покрытие кода тестами и тщательная верификация. Эти меры повышают стойкость ПО к аномалиям, хоть и не являются направленной киберзащитой.

- Специальные технические условия (Special Conditions). При сертификации новых самолётов или модернизации регуляторы вводят «спецусловия» по кибербезопасности. Например, совместная рабочая группа РФ, Якова и Миля разрабатывает требования обеспечения информационной безопасности бортовой техники [34]. В зарубежной практике к типовым сертификатам добавляются специальные требования по защите самолёта от кибератак [35], [36]. Европейское агентство (EASA) внедрило новый регламент ЕС 2023/203, обязывающий авиапроизводителей и авиакомпании учитывать риски информационной безопасности, влияющие на безопасность полётов. Кроме того, появляются стандарты, напрямую ориентированные на ИБ: так, разработка DO-326A/ED-202A (SC - 216 RTCA/EUROCAE) определяет процесс создания и сертификации авионики с учётом угроз (Airworthiness Security Process Specification). Этот документ требует, чтобы проектировщики идентифицировали угрозы и внедряли меры против атак уже на этапе проектирования воздушного судна.

- Сети и коммуникации. Для защиты воздушных сообщений рекомендуются методы шифрования и аутентификации. Например, для ADS-B и ACARS обсуждаются криптографические расширения и защищённые каналы. В некоторых новых системах авиакомпаний и приёмниках радио используются VPN-соединения или IPSec для шифрования связей между самолётом и диспетчером. Кроме того, практикуется сегментация сети внутри самолёта: отделение локальной пассажирской Wi-Fi сети от критических систем фильтрами и шлюзами (firewall), хотя полностью исключить паразитное соединение не всегда просто. Разработчики ARINC 823 (протокол загрузки данных) и ARINC 664 (AFDX-сеть) в рамках DO-178C предусматривают валидацию всех входящих данных, чтобы предотвратить переполнение буфера или подделку пакетов.

- Обнаружение вторжений (IDS/IPS). Интересной мерой являются системы обнаружения и предотвращения кибератак на борту. Например, Southwest Research Institute разработала ПО CyberDAMS (Cyber Detection And Mitigation System) для

самолётов [37]. Это решение на основе машинного обучения умеет быстро выявлять аномалии в поведении авионики и автоматически изолировать подозрительные компоненты. Подобные системы «заполняют разрыв» между традиционной безопасностью полётов и киберзащитой: они обучаются на нормальных полётных данных и в реальном времени отслеживают отклонения. Также в исследованиях предлагают внедрять IDS для анализа сигналов ADS-B (анализ последовательности принимаемых сообщений) и шумовых портов ACARS, чтобы распознавать подозрительные шаблоны. В сфере ATM (управления воздушным движением) появляются идеи совместной многоагентной системы обнаружения атак на командные каналы, основанные на сравнении данных с разных источников. Важную роль играют и «перехватчики» угроз: Национальный центр кибербезопасности Великобритании (NCSC) выдает рекомендации по защите, регулярно отслеживает угрозы и сотрудничает с авиапроизводителями и аэропортами при инцидентах, как, например, во время атаки на Collins Aerospace [38].

- Нормативы ICAO/EASA. На международном уровне вводятся стандарты, ориентированные на ИБ. ИКАО подготовила «План действий по обеспечению кибербезопасности в гражданской авиации» и включила соответствующие положения в сборники руководств ICAO Aviation Security Manual. EASA и FAA также включили требования к ИБ в свои руководства по летной годности: так, новые сертификаты предусматривают, чтобы «требования ИБ корабля соответствовали критериям летной годности» [39]. В частности, DO-356 (FAA AC 23.1309−1C) ставит задачу учитывать киберугрозы наравне с другими системными отказами при анализе безопасности.

В целом существующие подходы в авиации строятся на принципах «безопасность прежде всего»: все нововведения проверяются на предмет влияния на летную годность, а процессы разработки подкреплены строгим документированием. Тем не менее эксперты замечают, что кибербезопасность зачастую «не оставляют дыр в заборе»: её нужно рассматривать системно как часть общей безопасности полётов (safety/security merge) [40]. Основной упор сейчас делается на формализацию процессов (стандарты, тесты), однако реалии показывают необходимость оперативного обмена информацией об угрозах между государствами и компаниями, а также обучения специалистов по авиационной безопасности, которые знают особенности летных систем.

Количественная оценка киберрисков

Важным элементом современного подхода к кибербезопасности является количественная оценка рисков. В отличие от качественного анализа, где угрозы ранжируются по шкалам «низкая/средняя/высокая», количественные методы позволяют численно выразить вероятность реализации атак и потенциальный ущерб. В авиационной сфере такие оценки особенно значимы, поскольку они служат основой для принятия решений о внедрении защитных мер и распределении бюджетов.

Одним из распространённых подходов является использование матриц рисков, где вероятность атаки (например, на основе статистики инцидентов или экспертных оценок) умножается на величину возможного ущерба (финансовые потери, человеческие жертвы, репутационные риски). Более формализованные методы, такие как CVSS (Common Vulnerability Scoring System), адаптируются для оценки критичности уязвимостей в авионике: учитываются доступность вектора атаки, сложность эксплуатации,

необходимость физического доступа и влияние на безопасность полётов. Также применяется моделирование угроз (например, на базе STRIDE или Attack Trees), которое позволяет оценить вероятность успешной атаки с учётом существующих контрмер.

Для прогнозирования вероятностей используются статистические модели, включая байесовские сети и анализ временных рядов, которые обрабатывают данные о предыдущих инцидентах, частоте обновлений ПО, результатах пентестов и аудитов. В рамках требований DO-326A рекомендуется проводить количественную оценку рисков на этапе проектирования и периодически пересматривать её в процессе эксплуатации. Это позволяет, например, обосновать необходимость установки дополнительных IDS-сенсоров или перехода на шифрование ACARS. Внедрение таких практик в авиакомпаниях и у производителей способствует переходу от реактивного управления рисками к проактивному, где инвестиции в защиту распределяются в соответствии с объективной оценкой угроз.

В целом существующие подходы в авиации строятся на принципах «безопасность прежде всего»: все нововведения проверяются на предмет влияния на лётную годность, а процессы разработки подкреплены строгим документированием. Тем не менее эксперты замечают, что кибербезопасность зачастую рассматривают как дополнение, а не как неотъемлемую часть общей безопасности полётов (safety/security merge) [41]. Основной упор сейчас делается на формализацию процессов (стандарты, тесты), однако реалии показывают необходимость оперативного обмена информацией об угрозах между государствами и компаниями, а также обучения специалистов по авиационной безопасности, знакомых с особенностями лётных систем.

Перспективы угроз и защиты

Угрозы в авиации продолжают эволюционировать. На фоне обострения международных конфликтов государства и их специальных служб могут всё чаще прибегать к кибератакам на критическую инфраструктуру, к которой относят и гражданскую авиацию. Уже сейчас «сейлор» атаки, направленные на ИБ авиапарка и аэродромов, считаются одним из приоритетных направлений для подготовки спецслужб. К числу новых вызовов добавляются следующие тенденции:

- Рост автономности и дронов. Распространение БПЛА (дронов), летающих такси (eVTOL) и беспилотных грузоперевозок ведёт к увеличению количества «лёгких» воздушных судов с цифровыми управляемыми системами. Дроны могут работать в сетях (например, кооперация нескольких дронов), что создаёт новые точки доступа для взлома. Если в будущем массово внедрят дроны-пассажироперевозки, проблемы ИБ будет нужно решать не только для одного пилотируемого самолёта, но и для целых управляющих сетей. Автоматизация полётов (помимо существующего автопилота) будет опираться на ИИ – например, для расписания полётов, оптимизации маршрутов и мониторинга техники. Это означает, что алгоритмы планирования и диагностики полётов должны быть защищены от атак на целостность данных и моделей. В перспективе ожидается, что в авиации появятся системы адаптивной защиты на базе ИИ: самообучающиеся модули, постоянно обновляющие сигнатуры угроз и анализирующие аномалии. Уже сегодня тестируются нейросетевые IDS для протоколов ADS-B и ACARS (см. раздел выше), а в будущем это направление лишь усилится.

- Интернет вещей и «умный» самолёт. Самолёты всё больше соединяются с облаками и «интернетом вещей»: воздушные суда и компоненты передают телеметрию на наземные службы в реальном времени, что позволяет проводить предиктивное обслуживание. Однако это привносит угрозы удалённого вмешательства. Например, Airbus и Boeing исследуют системы киберзащиты, интегрированные в самолётные шлюзы связи, которые будут блокировать недостоверные данные. Кроме того, «умные» аэропорты – с системами автоматизации посадки и контроля доступа – также нуждаются в совместной защите: атака на аэропорт может косвенно отразиться на безопасности полётов (как очереди при регистрации).

- Международное сотрудничество. Поскольку авиация по определению трансгранична, киберугрозы требуют совместных усилий. Как подчёркивается в декларации ICAO, важно развивать обмен информацией о киберинцидентах между странами и отраслями. Создаются глобальные инициативы: например, ICAO разрабатывает методики оценки киберрисков в авиакомпании, а в Европе действует сеть CERT авиационных организаций. Важна унификация требований: если у одного регулятора строгие нормы по ИБ, а у другого нет, то в проектировании самолёта это создаёт дыры. Поэтому будущее – за глобальными стандартами (подобно ИСО 27000, NIST и т. д., адаптированными под авиацию) и скоординированными регламентами EASA/ICAO/FAA, чтобы самолёты и аэропорты разных стран могли безопасно взаимодействовать.

- Роль искусственного интеллекта в защите. С другой стороны, сами авиакомпании и регуляторы всё активнее используют ИИ для защиты. Это включает машинное обучение для анализа журналов бортовых компьютеров, прогнозирование вероятности атак на основе разведданных и т. д. Платформы «больших данных» (Big Data) настраиваются на сбор телеметрии полётов и помех, что помогает в автоматическом выявлении новых векторов атак. Уже сегодня кибер-мониторинг воздушного движения в Редмонде и НЦЦ США применяет алгоритмы для выявления аномалий (необычные сигналы ADS-B, подозрительные шаблоны радиообмена). В ближайшие годы ожидается, что ИИ будет не только обнаруживать, но и самостоятельно реагировать на некоторые инциденты (например, изолировать атакованные компоненты во время полёта).

Таким образом, сектор авиации должен готовиться к киберугрозам будущего так же серьёзно, как к физическим опасностям: требуется инвестировать в исследования, менять регламенты и создавать международные механизмы скоординированного реагирования. Отсутствие границ и высокая сложность современных воздушных систем делают необходимость совместных стандартов очевидной.

Заключение

В итоге было выявлено, что кибербезопасность авиационных систем представляет собой сложную и многогранную задачу, охватывающую как бортовую авионику воздушного судна, так и наземную инфраструктуру аэропортов, центры управления воздушным движением и информационные сервисы авиакомпаний. Цифровая трансформация авиационной отрасли значительно повысила уровень автоматизации, удобство эксплуатации и эффективность управления, однако одновременно открыла новые риски и уязвимости.

В частности, потенциальные слабые места могут возникать в беспроводных интерфейсах (Wi-Fi), каналах передачи служебных сообщений (ACARS), спутниковой навигации (GPS), а также во внутренних бортовых сетях передачи данных. При недостаточной защите такие элементы способны стать точками входа для злоумышленников и поставить под угрозу как процессы обслуживания пассажиров, так и элементы управления воздушным судном. Рассмотренные реальные инциденты, включая атаку на системы Collins Aerospace и технические сбои у «Аэрофлота», продемонстрировали, что киберинцидент способен парализовать работу авиаперевозчика столь же эффективно, как природная или техническая авария.

На основании проведённого анализа можно сделать вывод, что обеспечение безопасности должно начинаться ещё на этапе проектирования. Важную роль играет применение стандартов разработки программного обеспечения (например, DO-178C), принципов строгого разделения вычислительных сред (ARINC 653), а также регулярное тестирование и аудит систем на предмет уязвимостей. Существенное значение имеет внедрение систем постоянного мониторинга событий безопасности, обнаружения вторжений и анализа аномалий в сетевом трафике. Не менее важным направлением остаётся международное сотрудничество и координация усилий под эгидой таких организаций, как ICAO и EASA.

В дальнейшем основными вызовами для отрасли станут растущая взаимосвязанность систем, развитие облачных сервисов, расширение цифровых каналов взаимодействия между самолётом и наземной инфраструктурой, а также появление автономных и дистанционно управляемых платформ. Эти тенденции требуют перехода от реактивной модели защиты к превентивной, при которой информационная безопасность учитывается на всех этапах жизненного цикла авиационной техники — от разработки до эксплуатации и модернизации.

Авиаперевозчикам и производителям следует систематически оценивать киберриски, внедрять бортовые системы обнаружения вторжений (IDS), своевременно обновлять программное обеспечение с учётом актуальных угроз и уделять внимание обучению персонала основам кибербезопасности. На государственном уровне целесообразно гармонизировать нормативные требования, совершенствовать процедуры сертификации и поддерживать научные исследования в области защиты авиационных систем.

Реализация комплекса перечисленных мер позволит существенно снизить вероятность успешной кибератаки на авиационную инфраструктуру и обеспечит устойчивое и безопасное функционирование гражданской авиации в условиях дальнейшей цифровизации.

СПИСОК ЛИТЕРАТУРЫ

1. [2], [3], [4] ICAO. Muscat Declaration on Aviation Security and Aviation Cybersecurity. ICAO Security Week, Muscat, Oman, 11 December 2024. - https://www.icao.int/news/international-community-adopts-landmark-declaration-aviation-security-and-cybersecurity?utm_source=chatgpt.com
2. [1], [6], [12], [13], [34], [35], [36], [39], [40], [41] Kaspersky ICS CERT. Ошибки в цифровых системах авионики ставят под угрозу безопасность полётов (отчёт / аналитика Kaspersky ICS CERT). Moscow: «Лаборатория Касперского», 3 July 2025. - https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-Digital-avionics-systems-

errors-endanger-aviation-safety.pdf#:~:text=учитывать%20при%20оценке%20рисков%20кибербезопасности,Например%2C%20подобные%20планшеты

3. [5], [23], [25], [27] AP News. Cyberattack disrupts check-in systems at major European airports. 20 September 2025. - https://apnews.com/article/europe-airports-cyberattack-29b6d890baf7ac3a22f0f2b2f169b890
4. [7] [8] Ryanair flight diverted from Vilnius due to GPS interference, Lithuania says - https://www.reuters.com/business/aerospace-defense/ryanair-flight-diverted-vilnius-due-gps-interference-lithuania-says-2025-01-17/#:~:text=Ryanair%20did%20not%20immediately%20respond,a%20Reuters%20request%20for%20comment
5. [10], [11], [14], [19], [20], [21], [22] Researcher Successfully Hacked In-Flight Airplanes - From the Ground - https://www.darkreading.com/vulnerabilities-threats/researcher-successfully-hacked-in-flight-airplanes---from-the-ground
6. [9] Connected Aircraft Solution Architecture - Architecture Diagrams - https://docs.aws.amazon.com/pdfs/architecture-diagrams/latest/connected-aircraft-solution-architecture/connected-aircraft-solution-architecture.pdf#:~:text=,2
7. [15], [29], [30], [31] Атака на самолеты: сколько стоит удар хакеров по «Аэрофлоту» и тысячам пассажиров - https://www.forbes.ru/biznes/542815-ataka-na-samolety-skol-ko-stoit-udar-hakerov-po-aeroflotu-i-tysacam-passazirov
8. [16], [17] United Airlines bars security researcher from flight after tweet about hacking - https://www.theguardian.com/business/2015/apr/19/united-airlines-security-researcher-chris-roberts-hacking#:~:text=One%20World%20Labs%2C%20which%20tries,risks%20before%20they%20are%20exploited
9. [24] , [26], [28], [38] ENISA confirms ransomware behind airport disruptions; delays at Heathrow, Brussels, Berlin continue - https://industrialcyber.co/threats-attacks/enisa-confirms-ransomware-behind-airport-disruptions-delays-at-heathrow-brussels-berlin-continue/#:~:text=A%20third,in%20the%20European%20aviation%20sector
10. [33] DO-178C, Software Considerations in Airborne Systems and Equipment Certification - https://en.wikipedia.org/wiki/DO-178C#:~:text=DO,3
11. [37] Aircraft Cybersecurity- https://www.swri.org/markets/defense-security/defense-aerospace-aircraft/aircraft-engines-maintenance-testing/aircraft-cybersecurity#:~:text=CyberDAMS%20aircraft%20cybersecurity%20software%20detects,Features%20include

ТҮЙІНДЕМЕ

Авиация жүйелерінің киберқауіпсіздігі және қорғаныстың келешегі

Д.Н. Батырбеков

Қазақстан-Неміс Университеті
Алматы, Қазақстан

Мақалада авиациялық жүйелердің киберқауіпсіздігінің негіздері талданып, сала алдында тұрған негізгі сын-қатерлер мен міндеттер болжанады. Зерттеу нәтижесі авиациялық жүйелердің киберқауіпсіздігі — әуе кемесінің борттық авионикасынан бастап әуежайлардың жерүсті инфрақұрылымы, әуе қозғалысын басқару орталықтары және әуекомпаниялардың ақпараттық қызметтеріне дейін қамтитын күрделі әрі көпқырлы сала екенін көрсетті.
Түйінді сөздер: авиациялық жүйелердің киберқауіпсіздігі, кибертәуекелдер, сандық борттық жүйелер.

SUMMARY

CYBERSECURITY OF AVIATION SYSTEMS AND PROSPECTS FOR DEFENSE

D.N. Batyrbekov

Kazakh-German University
Almaty, Kazakhstan

The article analyzes the fundamentals of cybersecurity in aviation systems and forecasts the main challenges and tasks facing the industry. It reveals that cybersecurity in aviation systems is a complex, multifaceted domain encompassing both the onboard avionics of an aircraft and the ground infrastructure of airports, air traffic control centers, and airline information services.
Keywords: cybersecurity of aviation systems, cyber risks, digital onboard systems.

Автор: Батырбеков Диас Нурланулы - студент Казахстанско-Немецкий университета, факультет информационного инжиниринга в экономике

student.batyrbekov@dku.kz

+77772776244