Ошибки в цифровых системах авионики ставят под угрозу безопасность полетов

Василий Бузоверя

03.07.2025 Версия 1.0

Оглавление

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Введение

Гражданская авиация, как и многие другие отрасли, переживает цифровую трансформацию. Эта трансформация предполагает рост уровня информационной связности самолетов с наземной цифровой инфраструктурой и как результат ведет к новым рискам информационной безопасности (ИБ). Об этом упоминается, в частности, в руководстве по авиационной безопасности Международной организации гражданской авиации (ИКАО)[1].

В вопросе обеспечения информационной безопасности наиболее интересны бортовые системы, поскольку в воздушных судах предыдущих поколений они были изолированы от наземных систем и имели ограниченную и контролируемую связность между собой. Бортовые системы — цифровые системы авионики (от слов «авиация» и «электроника»), которые используются для выполнения различных задач в ходе полета, включая управление двигателем, навигацию, связь, взаимодействие с наземными службами. В этой статье под системами авионики мы понимаем именно цифровые бортовые системы или цифровые подсистемы бортовых систем. Все они интегрируются в комплекс бортового оборудования (КБО).

В связи с ростом уровня связности и открытости бортовых систем возникает потребность в их защите от кибератак — умышленного несанкционированного воздействия на системы по цифровым интерфейсам (электромагнитные и иные аналоговые воздействия кибератаками не являются). Кибератаки могут вызывать отказы систем авионики и приводить к авиационным событиям (инцидентам и происшествиям)[2].

В открытом доступе пока не появлялось сообщений о подтвержденных кибератаках на системы авионики или уязвимостях в них. Но инциденты и происшествия, связанные с ошибками в программно-аппаратном обеспечении таких систем, уже происходили. Анализ причин и последствий этих инцидентов может дать некоторое представление о

[1] Важные документы Международной организации гражданской авиации (ИКАО) для ознакомления:

- Резолюции 40-й сессии Ассамблеи ИКАО, 2019;
- Культура кибербезопасности в гражданской авиации, 2022;
- План действий по обеспечению кибербезопасности, 2022.

[2] К авиационным происшествиям относятся события, в результате которых были серьезно ранены или погибли люди, либо серьезно поврежден, потерян или полностью разрушен самолет. К авиационным инцидентам относятся все иные события, которые оказали или могли оказать негативное влияние на безопасность полета.
Источник: Annex 13 to the Convention on International Civil Aviation: Aircraft Accident and Incident Investigation, ICAO, Edition 11, July 2016.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

характере вероятных атак — сделать предположения о возможных уязвимостях цифровых систем авионики и последствиях их целенаправленной эксплуатации злоумышленниками, понимающими назначение систем, их технические особенности и слабые места.

Мы рассматриваем только авиационные события с гражданскими магистральными самолетами, которые в соответствии с принятой в отрасли классификацией относятся к самолетам транспортной категории (transport category airplanes — в США и large airplanes — в странах Евросоюза). Это, например, самолеты Boeing 787, Boeing 737, Airbus A350, Airbus A320, SSJ-100 (RRJ-95), MC-21, Comac C919. Однако приведенные примеры могут помочь при анализе рисков кибербезопасности воздушных судов различных типов, в том числе легких самолетов, вертолетов и беспилотных авиационных систем.

За рамками этой статьи остаются проблемы, касающиеся функций позиционирования, навигации и времени (Position, Navigation and Timing, PNT), в том числе связанные с технологиями спутниковой навигации (GPS, ГЛОНАСС) и протоколами автоматического обмена информацией с наземными службами (ADS-B и ACARS). Эти проблемы затрагивают вопросы взаимодействия бортовых и связанных с ними наземных и спутниковых систем и требуют отдельного рассмотрения, поэтому вынесем их за рамки данной статьи.

Современные цифровые комплексы бортового оборудования

Важными характеристиками комплексов бортового оборудования последнего (пятого) поколения[3] с точки зрения информационной безопасности являются высокая связность и открытость. Цифровые системы авионики подключены к единой бортовой вычислительной сети на основе протокола межсетевого взаимодействия IP (IP-протокола), при этом отдельные системы связаны с наземной информационной инфраструктурой авиакомпаний и аэропортов[4]. На рисунке 1 показаны некоторые цифровые системы самолета Boeing 787 Dreamliner — первого

[3] Комплекс бортового оборудования пятого поколения установлен, например, в таких самолетах, как Boeing 737 NG/MAX, Airbus A320neo, RRJ-95, MC-21.
[4] Иногда для обозначения самолетов с цифровыми системами авионики используются термины «воздушное судно на основе электронных технологий» (e-enabled aircraft) или «подключенное воздушное судно» (connected aircraft).

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«цифрового» самолета с КБО пятого поколения, который совершил свой первый коммерческий рейс в октябре 2011 года.

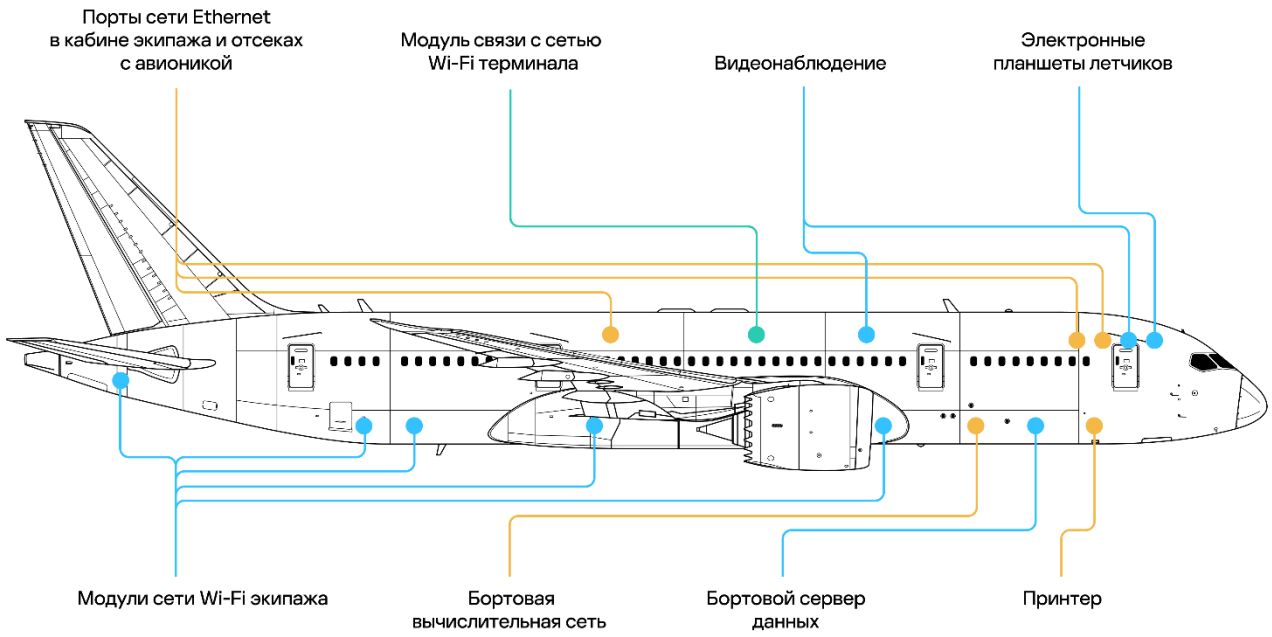

Рисунок 1. Цифровые бортовые системы самолета Boeing 787 Dreamliner

Еще одна важная особенность современных КБО состоит в том, что основные самолетные системы работают под управлением программного обеспечения. Например, самолет модели Airbus A350 XWB с КБО пятого поколения содержит 1200 программных компонентов (software parts). При этом в современных КБО наряду со специализированным используется программное и аппаратное обеспечение общего назначения.

Основные и дополнительные системы комплекса бортового оборудования

Системы комплекса бортового оборудования самолетов можно разделить на основные и дополнительные. Основные системы критичны для выполнения полета и обеспечения безопасности. К ним относятся, например, система энергоснабжения, система управления самолетом, система пожаротушения. Дополнительные системы не используются для управления самолетом и обеспечения безопасности, однако без них эффективная коммерческая эксплуатация практически невозможна. К таким системам относятся, например, бортовая информационно-

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

развлекательная система и переносной электронный планшет летчиков (ЭПЛ). В соответствии с российскими и зарубежными авиационными правилами[5] дополнительные системы не должны представлять опасность и негативно воздействовать на основные системы. Переносные устройства не являются частью сертифицированной типовой конструкции.

Примечание 1. Электронные планшеты летчиков и техников

С помощью электронных планшетов летчиков экипаж получает необходимую для полета информацию, в том числе навигационные данные (карты и схемы, включая схемы заходов на посадку), метеосводки и руководства по эксплуатации. При их использовании наличие на борту соответствующей бумажной документации необязательно.

На электронные планшеты летчиков устанавливаются приложения для расчета параметров полета, например, взлетно-посадочных характеристик, взлетной массы и центровки самолета, запаса топлива.

Электронные планшеты летчиков бывают двух видов: стационарные устройства, интегрированные в КБО, и переносные подключаемые устройства. Первые разрабатываются в соответствии с требованиями к авиационной технике, вторые создаются на основе готовых коммерческих продуктов вроде Apple iPad. На рисунке 2 пилот использует электронный планшет на основе Apple iPad с запущенным приложением Flysmart+[6].

К дополнительным переносным устройствам относятся также электронные планшеты бортпроводников и техников. Они отличаются от ЭПЛ лишь набором приложений. Специализированные приложения могут устанавливаться и через обычный магазин приложений (такой как Apple Store).

[5] Авиационные правила, часть 21 (сертификация авиационной техники):

- Федеральные авиационные правила «Сертификация авиационной техники, организаций разработчиков и изготовителей авиационной техники. Часть 21». Министерство транспорта Российской Федерации, 2014;
- The Code of Federal Regulations: Title 14 — Aeronautics and Space, Chapter I — Federal Aviation Administration, Department of Transportation, Subchapter C — Aircraft, Part 21 — Airworthiness Standards: Transport Category Airplanes, U.S. Government Publishing Office, 2022;
- Easy Access Rules for Airworthiness and Environmental Certification (Regulation (EU) No 748/2012), Part 21 (IR + AMC & GM), European Union Aviation Safety Agency (EASA), EASA eRules, May 2023.

[6] Технические сведения о приложении Flysmart+, разработанном компанией Navblue Inc., дочерним предприятием Airbus (Flysmart+ в Apple Store).

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Несмотря на то, что переносные электронные планшеты летчиков официально имеют низкий класс опасности, ошибки в их проектировании, реализации и использовании могут привести к серьезным последствиям. Так, в 2023 году в iOS были выявлены серьезные уязвимости нулевого дня (CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990), которые использовались в целевой кибератаке на устройства, работающие под управлением этой операционной системы. Об этом писали эксперты «Лаборатории Касперского»[7]. В том же году в приложении Flysmart+ была найдена уязвимость, информация о которой была доведена до разработчика в рамках ответственного раскрытия.

Рисунок 2. Электронный планшет летчиков на основе устройства Apple iPad

[7] Больше статей экспертов «Лаборатории Касперского» о кампании «Операция Триангуляция».

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Примеры инцидентов, связанных с отказами цифровых систем авионики

Исследователи кибербезопасности начали обращать внимание на отказы бортовых электронных (цифровых) систем еще в конце прошлого века. Уже тогда высказывались предположения о возможности возникновения таких отказов в результате кибератак. На протяжении многих лет в издании ACM SIGSOFT Software Engineering Notes в рубрике «Риски для общества из-за компьютеров и связанных с ними систем» (Risks to the Public in Computers and Related Systems) публикуются статьи об инцидентах и происшествиях, связанных с использованием компьютеров и компьютеризированных технических систем, в том числе систем авионики. В 1997 году бессменный редактор рубрики Питер Нойман выступил на международной конференции по авиационной безопасности, организованной комиссией правительства США по безопасности, с программным докладом о перспективных задачах в области авиационной кибербезопасности. Он отметил, что многие авиационные события, связанные с ошибками в авионике, могли бы быть вызваны и кибератаками, и призвал уделять больше внимания защите наземных и бортовых систем, особенно от масштабных скоординированных атак.

В этой статье мы приводим шесть примеров ошибок как в основных, так и в дополнительных системах КБО. Первые два касаются ошибок в переносных электронных планшетах летчиков. Последующие три — программно-аппаратных ошибок в основных системах авионики самолетов с современными КБО, реализующими концепцию интегрированной модульной авионики. Эти случаи примечательны тем, что в качестве временной меры для предотвращения отказов периодически выполнялся аппаратный сброс и перезагрузка систем путем выключения и включения электроснабжения самолета. А в последнем примере речь идет об ошибке в бортовых регистраторах, из-за которой регистрировались неверные параметрических данные.

Хронология рассмотренных ошибок и связанных с ними событий приведена на рисунке 3.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

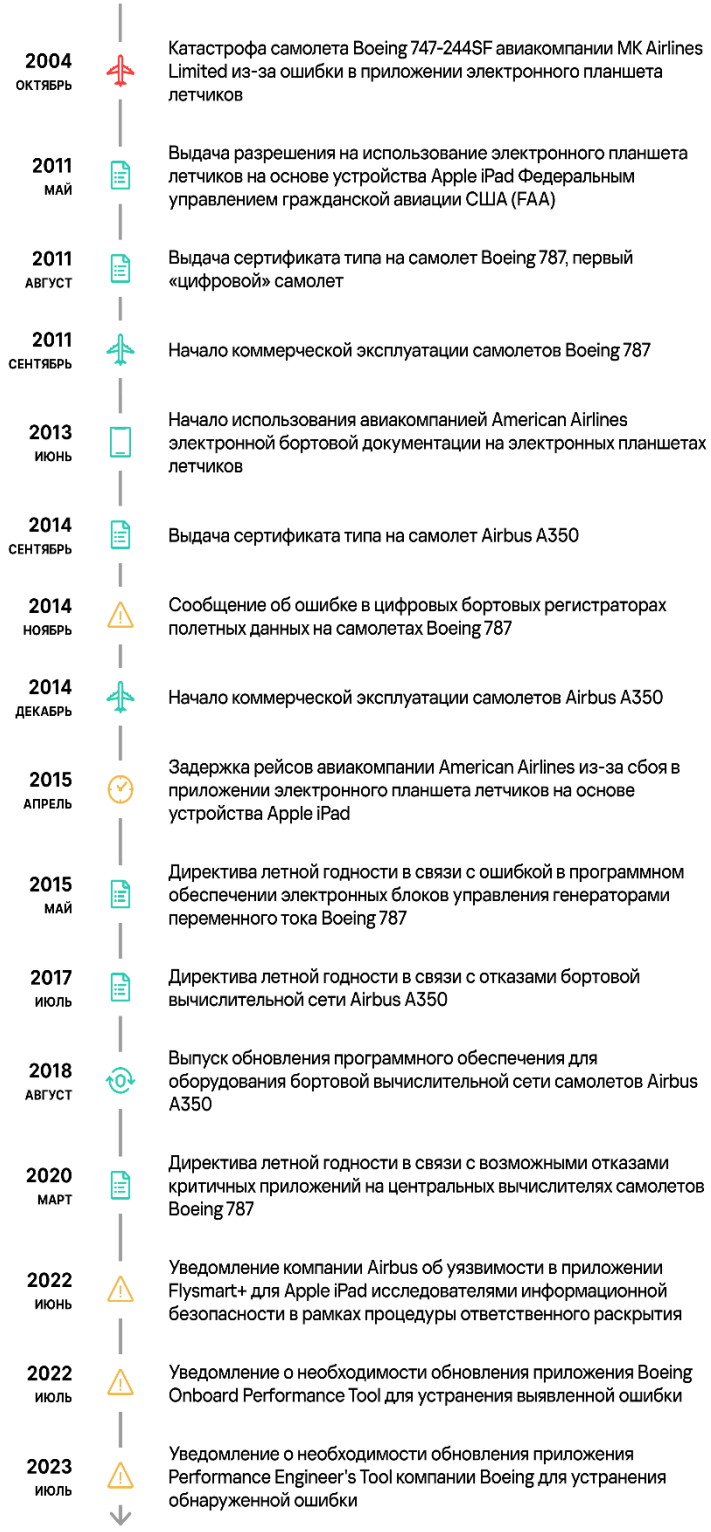

Рисунок 3. Хронология рассмотренных событий

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Задержка рейсов авиакомпании American Airlines

Вечером 28 апреля и утром 29 апреля 2015 года десятки рейсов авиакомпании American Airlines были задержаны в нескольких аэропортах в США из-за проблем с приложением на электронных планшетах летчиков на основе устройств Apple iPad. Пассажиры сообщили в социальных сетях о задержках рейсов из аэропортов Далласа, Нью-Йорка, Лос-Анджелеса и Чикаго. В некоторых случаях задержка составила более трех часов. Все рейсы должны были выполняться на самолетах Boeing 737.

Представитель авиакомпании заявил, что всего было задержано 74 рейса: 24 — 28 апреля и 50 — 29 апреля. American Airlines, на тот момент крупнейшая авиакомпания в мире, выполняла в среднем 6700 рейсов в сутки. Согласно финансовому отчету компании за 2014 год она эксплуатировала 928 самолетов, 246 (27%) из которых были Boeing 737. То есть проблема затронула 8% флота авиакомпании.

Сбой программного приложения для электронных планшетов летчиков привел к тому, что экипажи не могли получить доступ к необходимым для полета навигационным картам и схемам. Ранее American Airlines полностью перешла на использование электронных версий навигационных документов на электронных планшетах летчиков вместо бумажных[8] на всех самолетах, укомплектованных этими устройствами.

Причиной сбоя приложения Boeing Onboard Performance Tool, разработанного компанией Jeppesen, стала программная ошибка. Jeppesen, подразделение Boeing, является ведущим мировым поставщиком аэронавигационных карт и схем. Как сообщило издание Avionics International со ссылкой на представителя Jeppesen, проблема затронула только специальную версию приложения, используемую авиакомпанией American Airlines, и не повлияла на работу других версий.

Ошибка возникла при обработке файла со схемой посадки в Вашингтонском национальном аэропорту имени Рональда Рейгана. В базу данных электронных карт и схем на электронных планшетах летчиков был загружен новый файл с обновленной схемой посадки, который имел такие же имя и идентификатор, как и файл с действующей схемой. В итоге на устройствах оказались две разные по содержанию копии одного файла. При попытке открыть этот файл приложение переставало работать.

[8] Авиакомпания American Airlines — первая авиакомпания, получившая разрешение регулятора (FAA) на использование на всех этапах полета электронной документации на переносных ЭПЛ вместо соответствующей бумажной документации.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Для устранения неисправности экипажам было рекомендовано переустановить навигационное приложение на планшетах. В некоторых случаях для этого самолеты пришлось вернуть с летного поля к терминалам, чтобы пилоты смогли подключиться к Wi-Fi-сети аэропорта. Кроме того, экипажи могли получить в аэропорту бумажные распечатки карт и схем. Вскоре вышло обновление приложения, которое устранило ошибку с загрузкой файла. До установки обновления, в качестве временной меры, на планшеты можно было загрузить схему Вашингтонского национального аэропорта имени Рональда Рейгана в формате PDF.

Дубликат файла появился на устройствах в ходе стандартной процедуры авиакомпании: новые схемы посадки загружались на планшеты за сутки до начала их использования, чтобы экипажи успевали ознакомиться с ними. При этом старые схемы продолжали действовать еще сутки. 28 апреля 2015 года в 19:00 по центральноамериканскому времени на планшетах экипажей появился файл с новой схемой посадки, что привело к одновременному сбою многих устройств в различных аэропортах. Первыми с проблемой столкнулись те пилоты, у которых Вашингтонский национальный аэропорт имени Рональда Рейгана был сохранен в списке избранных.

Следует отметить, что все изменения в навигационные сведения, в том числе в схемы посадки, вносятся в соответствии с процедурой регулирования и контроля аэронавигационной информации (Aeronautical Information Regulation and Control, AIRAC) ИКАО и вступают в силу в заранее установленные даты. Список дат определяется на несколько лет вперед и доступен на ресурсах ИКАО и регуляторов. Это всегда четверг, а интервал между соседними датами составляет 28 дней. Точное время вступления изменений в силу определяется национальным регулятором, в США это 09:00 по гринвичскому времени (с полуночи до четырех часов утра по местному времени в зависимости от часового пояса). В апреле 2015 года очередная дата в графике AIRAC выпала на 30-е число. Как видно, загрузка файла с новой схемой посадки произошла накануне.

В открытых источниках не сообщалось о причинах возникновения ошибки, в том числе о том, почему она была связана с конкретным файлом, не была выявлена ранее и затронула только версию программы для American Airlines. Оценки ущерба от инцидента также не приводилось, но его можно примерно рассчитать на основе доступной информации. Сбой привел к задержке 74 рейсов (примерно 1% от общего количества ежедневных рейсов авиакомпании), некоторые задержки превысили три часа. Учитывая среднюю загруженность рейсов American Airlines в апреле 2015 года

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

(81,6%) и среднюю пассажировместимость самолетов Boeing 737 в ее флоте (150 мест — в конце 2014 года и 159 мест — в конце 2015 года), можно предположить, что с задержками рейсов столкнулись около 10 тыс. пассажиров. Для авиакомпании такого масштаба (авиакомпания перевозит более 100 млн пассажиров в год) ущерб можно считать незначительным. Тем не менее, этот пример показывает, что подобные ошибки могут затрагивать большое количество самолетов в разных точках и часовых поясах, создавая трудности для операционной деятельности авиакомпании.

Проблемы, похожие на эту, могут возникать из-за нарушения целостности и доступности программного обеспечения и данных электронных планшетов летчиков и бортовой информационной системы. Это следует учитывать при оценке рисков кибербезопасности.

Отметим, что электронные планшеты летчиков работали на устройствах Apple iPad под управлением iOS. На основе этих устройств разрабатываются многие модели ЭПЛ. Например, подобные планшеты использует авиакомпания Delta, обладающая вторым по величине флотом в мире (975 магистральных самолетов в эксплуатации по состоянию на конец 2024 года).

Переносные электронные планшеты летчиков, включая установленное на них системное и прикладное программное обеспечение, не требуют сертификации регуляторами. За качество, надежность и защищенность таких устройств отвечают авиакомпании и их поставщики. Этот инцидент напоминает о важности управления отношениями с поставщиками в контексте комплексного обеспечения кибербезопасности.

Катастрофа самолета Boeing 747-244SF авиакомпании MK Airlines Limited

В октябре 2004 года в международном аэропорту Галифакс-Стэнфилд (провинция Новая Шотландия, Канада) при взлете из-за недостаточной тяги двигателей потерпел крушение грузовой самолет Boeing 747-244SF авиакомпании MK Airlines Limited. Все семь членов экипажа погибли.

В результате расследования катастрофы было установлено, что причиной стало неправильное определение экипажем взлетных характеристик самолета из-за использования при расчетах неверного значения взлетного веса. Для расчетов применялось специальное программное приложение на устройстве Boeing Laptop Tool, представляющем собой электронный планшет летчиков на основе ноутбука.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Согласно отчету Совета по безопасности на транспорте Канады (отчет A04H0004), опубликованному в июне 2006 года, наиболее вероятной основной причиной катастрофы стала особенность программного приложения на электронном планшете летчиков: оно автоматически, без уведомления пользователя, копировало значение взлетного веса из формы расчета веса в форму расчета взлетно-посадочных характеристик, даже если пересчет взлетного веса не производился (в таком случае копировалось ранее вычисленное значение). На рисунке 4 показана форма расчета взлетно-посадочных характеристик этого приложения.

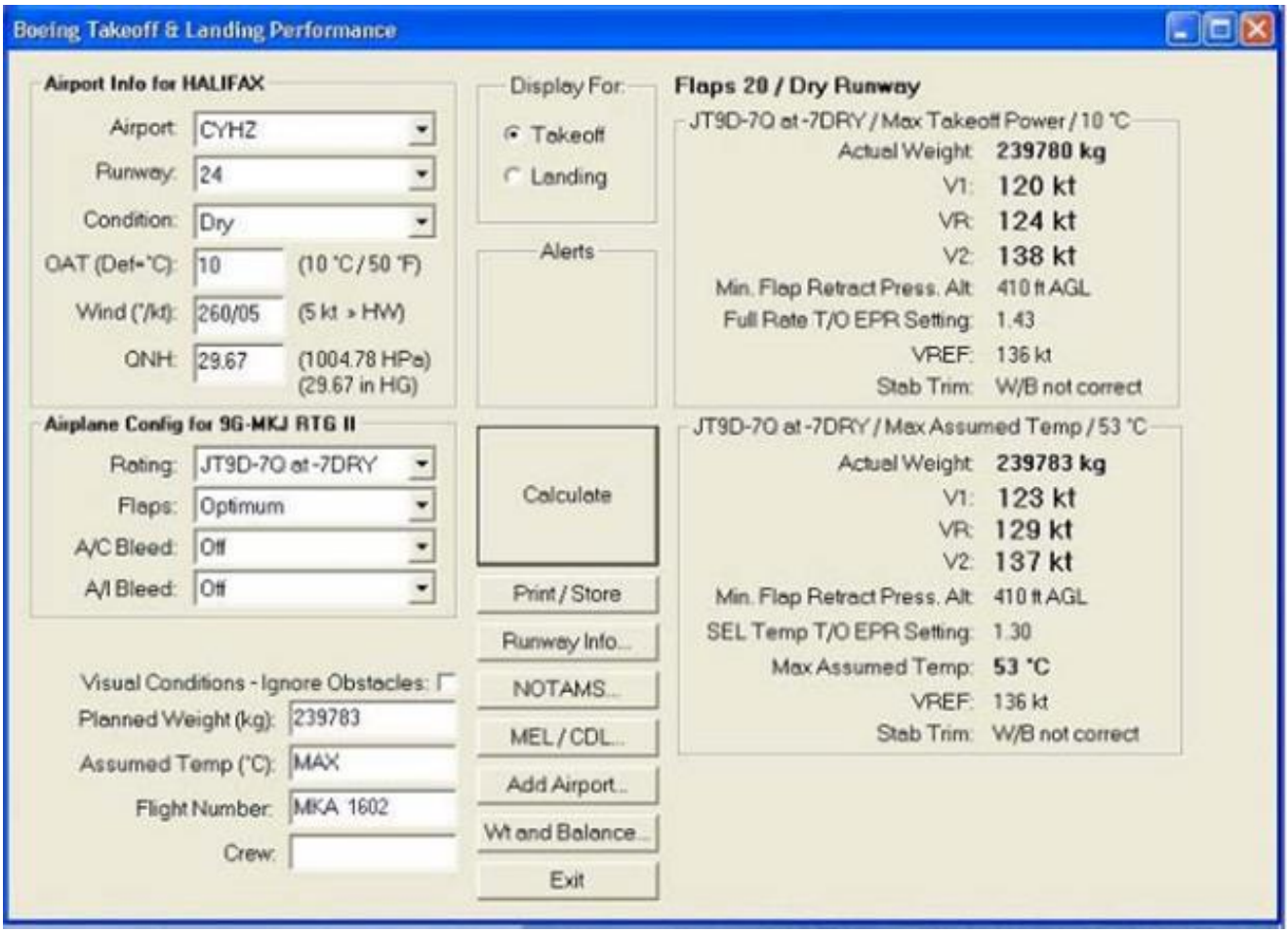

Рисунок 4. Форма расчета взлетных характеристик в приложении для устройства Boeing Laptop Tool[9]

[9] Скриншот формы расчета взлетных характеристик в приложении для устройства Boeing Laptop Tool взят из отчета Совета по безопасности на транспорте Канады.
Источник: Transport Safety Board of Canada. Aviation Investigation Report A04H0004. Reduced Power at Take-off and Collision with Terrain, MK Airlines Limited, Boeing 747-244SF 9G-MKJ, Halifax International Airport, Nova Scotia, 14 October 2004.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Из-за этой особенности приложения перед вылетом из аэропорта Галифакса для расчета взлетных характеристик использовалось значение взлетного веса для предыдущего сегмента полета из международного аэропорта Брэдли в Виндзор Локс (Коннектикут, США) в Галифакс. Расследование показало, что ошибка в исходных данных для расчета взлетных характеристик привела к катастрофе по ряду причин. Одна из них — отсутствие проверки вычислений, предписанной стандартными эксплуатационными процедурами авиакомпании. Независимо от этого, выявленная особенность приложения должна считаться ошибкой или недостатком[10]. Такие ошибки в человеко-машинных интерфейсах необходимо учитывать при оценке угроз и рисков информационной безопасности.

В отчете указано, что на момент происшествия не существовало методик или систем для оповещения экипажа о недостаточном ускорении самолета при взлете. С учетом этого обстоятельства Совет по безопасности на транспорте Канады рекомендовал авиационным регуляторам в сотрудничестве с ИКАО установить требование по оснащению самолетов системой мониторинга взлетных характеристик и оповещения экипажа о несоответствии параметров допустимым значениям. Рекомендаций относительно процедур или устройств для расчета взлетно-посадочных характеристик не приводилось.

Ошибки в реализации и использовании программного приложения на электронном планшете летчиков привели к катастрофе: погибли люди, самолет и груз были потеряны. Регулирующие органы выдали авиакомпании предписания обновить эксплуатационные процедуры. Примечательно, что согласно существующим авиационным правилам и руководствам считается, что переносные электронные планшеты летчиков не могут влиять на безопасность полета. То есть в этом случае фактический ущерб не соответствовал ожидаемому (потенциальному).

Примечание 2. Ошибки в приложениях компании Boeing для электронных планшетов

В связи с ошибкой в программе для вычисления взлетных характеристик на электронном планшете летчиков, которая привела к крушению самолета Boeing 747 авиакомпании MK Airlines Limited, следует обратить внимание на похожие ошибки, выявленные недавно.

[10] Werfelman, L. Fatal Calculation: Bad Weight Computation Dooms Takeoff // Aviation Safety World. Volume 1, Issue 4 (October 2006). – P. 18–24.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В июле 2023 года компания Boeing выпустила уведомление безопасности SAFO 23004 (Safety Alert for Operators) для эксплуатантов самолетов Boeing 737 (модели до семейства NG), Boeing 747, Boeing 757, Boeing 767. В нем сообщалось о необходимости обновления программного обеспечения Performance Engineer's Tool для устранения ошибок в вычислении максимального взлетного веса, которые могли приводить к недостаточной тяге двигателей при взлете. И хотя эти самолеты оснащены комплексом бортового оборудования предыдущего поколения, для их эксплуатации используются современные информационные системы.

Годом ранее, в июле 2022 года, компания Boeing выпустила уведомление безопасности SAFO 22002 для пользователей приложения Boeing Onboard Performance Tool на устройствах под управлением iOS. Приложение разработано компанией Jeppesen и используется в самолетах Boeing всех типов. В уведомлении сообщалось о двух ошибках, выявленных в одной из версий приложения, которые в определенных случаях вызывали сбои в его работе. В результате при расчетах взлетно-посадочных характеристик использовались неверные длины взлетно-посадочных полос: в одном случае это были параметры полосы аэропорта вылета вместо аэропорта назначения, в другом — полная длина взлетно-посадочной полосы, даже если взлет начинался не с начала полосы, а с ее пересечения с рулежной дорожкой. В обоих случаях экипаж получал неверные значения дистанций, что критично для безопасности полета. Пользователям рекомендовалось либо следовать специальным инструкциям для предотвращения сбоев в приложении, либо установить его обновленную версию, в которой эти проблемы были устранены.

Все типы располагаемых дистанций классифицируются в гражданской авиации как критические данные с точки зрения целостности данных.

В отчете указано, что из-за использования неверных значений взлетных характеристик уже происходили подобные авиационные события, в том числе катастрофы с жертвами. Упоминалось 12 событий, четыре из которых произошли в течение трех лет до рассмотренной катастрофы, причем два из них с участием самолетов Boeing 747 — с разницей в один день. В одном из этих инцидентов самолет Boeing 747-300 авиакомпании South African Airways получил повреждение при взлете (произошло касание взлетной полосы хвостовой частью) из-за того, что бортовой инженер использовал неверное значение взлетного веса при расчете взлетных характеристик с помощью электронного планшета. В другом случае самолет Boeing 747-412 авиакомпании Singapore Airlines тоже задел хвостом взлетную полосу. Это произошло из-за нехватки тяги и

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

критически низкой начальной скорости взлета. Пилоты ввели в систему самолетовождения неверно вычисленные значения взлетных характеристик. Несмотря на то, что цифры существенно расходились со значениями, вычисленными самой системой, она приняла их без предупреждения о возможной ошибке.

Проблема использования неверных взлетных характеристик известна давно и обсуждается уже несколько десятилетий. После пары инцидентов, произошедших в 2004 и 2006 годах из-за ошибок в расчетах, специалисты лаборатории прикладной антропологии Университета Париж Декарт провели исследование причин таких ошибок по заказу французских правительственных агентств — Бюро по расследованию и анализу безопасности гражданской авиации (BEA) и Главного управления гражданской авиации (DGAC). Результаты этого исследования легли в основу дальнейших работ на эту тему. Так, в 2011 году Бюро транспортной безопасности Австралии (ATSB) выпустило отчет об ошибках при расчетах и вводе взлетно-посадочных характеристик, а в 2012 году аналогичное исследование провело Национальное аэрокосмическое агентство США (NASA). В сентябре 2021 года Европейское агентство авиационной безопасности (EASA) опубликовало информационный бюллетень на тему использования ошибочных взлетных характеристик, ссылаясь на эти три исследования.

Результаты этих исследований свидетельствуют, что экипажи довольно часто допускают ошибки при расчетах взлетных характеристик или при вводе значений в систему самолетовождения (Flight Management System, FMS). Очевидно, существуют специфичные риски, связанные с использованием для таких расчетов электронных планшетов летчиков и подобных устройств. Например, в отчете NASA ошибки, возникающие при использовании экипажем планшетов для расчета взлетно-посадочных характеристик, выделены в отдельную категорию.

Примечание 3. Нарушение работы электронных планшетов летчиков под воздействием низких температур

В отчете Национального аэрокосмического агентства США (NASA), посвященном исследованию причин ошибок в расчетах взлетно-посадочных характеристик, упоминается случай с использованием ноутбука, который подвергся воздействию низких температур (cold-soaked). Несмотря на то, что пилоты ввели корректные данные, результаты расчетов оказались неверными. Экипаж не заметил ошибку, в итоге при разгоне начался неуправляемый подъем и взлет пришлось прервать на высокой скорости.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В современных комплексах бортового оборудования программные приложения для расчета взлетно-посадочных характеристик устанавливаются на серверах приложений бортовых информационных систем, встроенных и переносных электронных планшетах летчиков.

Большинство авиационных происшествий с человеческими жертвами происходит при взлете, начальном наборе высоты, заходе на посадку и посадке. По данным компании Boeing, за период с 2013 по 2022 год около 67% всех происшествий с жертвами произошли именно на этих этапах, хотя суммарная продолжительность этих этапов составляет лишь 6% от общего времени полета. В ежегодном аналитическом отчете компании Airbus также отмечается, что заход на посадку и сама посадка являются наиболее сложными этапами полета. Они характеризуются повышенной рабочей нагрузкой на экипаж и высокой вероятностью возникновения непредвиденных условий. В совокупности эти факторы могут приводить к опасным ситуациям.

Основным источником навигационной информации и данных о взлетно-посадочных характеристиках для экипажей служат электронные планшеты летчиков. Нарушение работы планшетов, удаление или искажение хранящейся на них информации на критических этапах полета могут значительно усложнить работу экипажа. Некоторые исследователи кибербезопасности считают, что кибератаки на приложения с данными для расчета взлетно-посадочных характеристик могут приводить к опасным ситуациям.

На основании вышеизложенного можно сделать вывод, что ошибки в системах, отвечающих за расчет взлетно-посадочных характеристик, даже если сами по себе эти ошибки не приводят к нежелательным последствиям, следует рассматривать как слабые места и предполагать, что злоумышленники могут использовать их.

Ошибка в программном обеспечении генераторов переменного тока самолетов Boeing 787

В мае 2015 года Федеральное управление гражданской авиации США (FAA) выпустило директиву летной годности[11] (FAA-2015-0936), согласно которой эксплуатанты самолетов Boeing 787 обязаны регулярно (не реже одного

[11] Директива летной годности — документ, издаваемый регулятором в случае выявления снижения уровня безопасности полетов. Содержит описание угрозы безопасности полетов и предписания по выполнению действий, направленных на восстановление достаточного уровня безопасности полетов.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

раза в 120 дней) полностью отключать электропитание самолета для предотвращения опасной ситуации, связанной со сбоем электронных блоков управления генераторами переменного тока (Generator Control Unit). Отключать питание необходимо было не менее, чем на 15 секунд (cold and dark state), при этом отсоединять аккумуляторные батареи — на борту их две — не требовалось.

Лабораторные тесты компании Boeing (производитель и держатель сертификата типа самолета) выявили ошибку в программном обеспечении блоков управления генераторами: через 248 дней непрерывной работы генератора происходило переполнение программного счетчика, и каждый из шести генераторов самолета переключался в безопасный режим работы (failsafe mode) независимо от этапа полета. Генерация переменного тока при этом прекращалась, что могло привести к потере управления самолетом. Таким образом, ошибка в программном обеспечении электронного блока управления генератором могла вызвать катастрофическое отказное состояние на уровне самолета[12].

На момент публикации директивы в эксплуатации в США было зарегистрировано 28 самолетов Boeing 787, на которые распространялись требования документа (по всему миру эксплуатировалось более 100 самолетов). По оценкам Федерального управления гражданской авиации США (FAA), стоимость одного цикла отключения и повторного включения электроснабжения самолета, учитывая только стоимость нормо-часа технического обслуживания, составляла 85 долларов.

В уведомлениях операторам Boeing сообщал, что выпуск обновления программного обеспечения планировался на четвертый квартал 2015 года. В октябре 2018 года была выпущена новая директива летной годности (FAA-2017-0771), требовавшая установки обновленного программного обеспечения блоков управления генераторами, что отменяло действие предыдущей директивы. Таким образом, полное устранение выявленной ошибки, способной привести к серьезному отказу, заняло более трех лет.

Федеральное управление гражданской авиации США (FAA) оценивало стоимость работ по обновлению программного обеспечения, учитывая только стоимость нормо-часа, в 510 долларов на один самолет. Работы

[12] К катастрофическим отказным состояниям на уровне самолета относятся все состояния самолета, которые возникают вследствие отказов и препятствуют продолжению безопасного полета и посадке.
Источники:

- ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE International, December 01, 1996.
- Р-4761: Руководство по методам оценки безопасности систем и бортового оборудования воздушных судов гражданской авиации, Межгосударственный авиационный комитет, Авиационный регистр, 2010.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

включали непосредственно установку программного обеспечения и операции по отключению и повторному включению электроснабжения. Дополнительно требовались другие работы, стоимость которых с учетом только нормо-часа технического обслуживания была оценена в 1360 долларов на один самолет. На момент выхода директивы в США было зарегистрировано 55 самолетов, на которые она распространялась. Обновленное программное обеспечение компания Boeing предоставляла бесплатно, однако работу по его установке оплачивали авиакомпании-эксплуатанты, так как она не покрывалась гарантией.

На основании приведенных в директивах оценок стоимость всех работ по устранению ошибки для эксплуатантов могла составлять около 1500 долларов на каждый самолет. Сумма небольшая, но она не включает затраты разработчика на создание и сертификацию обновления программного обеспечения.

В данном случае обошлось без авиационного инцидента, но этот пример показывает, что устранение ошибок в системах авионики может занимать длительное время — и это нужно обязательно учитывать при оценке рисков кибербезопасности.

Ошибка программных приложений центрального вычислителя самолетов Boeing 787

В марте 2020 года Федеральное управление гражданской авиации США (FAA) издало директиву летной годности (FAA-2020-0205), согласно которой эксплуатанты самолетов Boeing 787 обязаны регулярно (не реже одного раза в 25 дней) полностью отключать электропитание самолета. Директива основана на сервисном бюллетене компании Boeing (B787-81205-SB420045-00) и направлена на предотвращение катастрофических отказных состояний на уровне самолета из-за скрытого частичного отказа[13] центрального вычислителя. В бюллетене говорится, что проблема была выявлена в ходе внутреннего анализа и тестирования. Нам не удалось найти сообщений об отмене директивы.

На момент выпуска директивы в США были зарегистрированы 196 самолетов, на которые распространялись ее требования. С учетом только стоимости нормо-часа на техническое обслуживание Федеральное

[13] Скрытый частичный отказ — частичное нарушение работоспособности системы, которое не обнаруживается визуально или штатными методами и средствами контроля и диагностирования, но может быть выявлено при проведении технического обслуживания или специальными методами диагностирования. При полном отказе система переходит в нерабочее состояние.
Источник: ГОСТ 27.002–2015 Надежность в технике. Термины и определения, 2016.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

управление гражданской авиации США (FAA) оценивало стоимость необходимых работ (цикл отключения и включения электропитания самолета) в 85 долларов на один самолет. Таким образом, общие расходы, связанные с выполнением директивы, за год составляют примерно 1275 долларов на один самолет. Впрочем, есть мнение, что «перезагрузка» самолетов обычно выполняется не реже раза в неделю, и в таком случае не возникает дополнительных расходов, связанных с выполнением требований директивы.

Центральный вычислитель (бортовая центральная вычислительная система) самолетов Boeing 787 называется Common Core System (CCS). На его основе реализована концепция интегрированной модульной авионики. На CCS выполняются программные приложения, реализующие критически важные для полета функции, такие как самолетовождение, навигация, управление шасси и другие. Ошибка может привести к катастрофическим отказным состояниям.

Обмен данными между программными приложениями на CCS и системами авионики осуществляется по бортовой вычислительной сети стандарта ARINC 664 Avionics Full-Duplex Switched Ethernet[14], которая в самолете Boeing 787 называется Common Data Network (CDN). На сетевом уровне применяется протокол IP, на транспортном — протокол UDP. Физический уровень передачи данных стандарта Ethernet в сети CDN реализуется на основе готовых коммерческих продуктов (Commercial Off-the-Shelf, COTS), логический — с помощью специализированных интегральных схем (Application Specific Integrated Circuit, ASIC). В самолете Boeing 787 на логическом уровне для проверки целостности и времени отправки сообщений используется протокол собственной разработки Boeing — Error Detection Encoding (EDE)[15], представляющий собой расширение средств контроля целостности сообщений протокола ARINC 664. Структура поля данных пакета UDP при использовании протокола EDE представлена в таблице 1.

[14] См. стандарт ARINC 664P7: ARINC Specification 664P7. Aircraft Data Network, Part 7, Avionics Full-Duplex Switched Ethernet Network, Aeronautical Radio, Inc., 2009, 150 p. Сети этого стандарта иногда называют сетями AFDX (AFDX — зарегистрированная торговая марка компании Airbus).

[15] См. спецификации и статьи:

- MX Foundation 4 API, ARINC 664 Frames, Max Technologies Inc. (Updated 10/23/2023);
- Santamarta, R. A Reverse Engineer's Perspective on the Boeing 787 '51 Days' Airworthiness Directive, IOActive, May 6, 2020;
- AMCX-FDX-2, 2 Port 10/100/1000Mbit/s, AFDX®/ARINC664P7, Test, Simulator and Monitor, Module for PMC, Data Sheet, AIM, 2023.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Длина поля, байт	Название поля
2	Порядковый номер EDE
6	Метка времени EDE
Переменная	Данные
2	Контрольная сумма CRC-X
2	Контрольная сумма CRC-Y (с учетом CRC-X)

Таблица 1. Структура поля данных пакета UDP при использовании протокола EDE

В директиве и бюллетене указывается, что после 51 дня непрерывной работы сервера CCS происходит несигнализируемое (скрытое) отключение функции проверки меток EDE. Если при этом также произойдет скрытый отказ коммутатора сети CDN, то на вход приложений на центральном вычислителе CCS могут поступать устаревшие данные. Например, на основных экранах обоих пилотов могут отображаться неверные значения критических для безопасности полета параметров (высота, скорость, показания авиагоризонта, параметры работы двигателя и др.), при этом сигнализации о сваливании и превышении скорости не будет. Пилоты будут управлять самолетом, используя неверные данные. В такой ситуации безопасный полет и посадка затруднены, то есть возникает катастрофическое отказное состояние. Вероятность скрытого отказа сетевого коммутатора CDN в директиве оценивается как крайне маловероятная. То есть вероятность возникновения катастрофического отказного состояния после 51 дня непрерывной работы сервера CCS также крайне маловероятная. Это на два порядка выше допустимого значения, поскольку согласно авиационным правилам и руководствам наступление катастрофического отказного состояния должно быть практически невероятным. Более того, возникновение такого состояние возможно из-за единичного отказа, что недопустимо.

Примечание 4. Вероятности отказных состояний

Крайне маловероятное (extremely remote) отказное состояние — отказное состояние, наступление которого не ожидается для одного конкретного самолета данного типа за весь срок его службы. Однако оно может возникнуть несколько раз в течение эксплуатации всех самолетов этого типа. Вероятность составляет 10^{-5} или менее, но более, чем 10^{-7} на час полета средней продолжительности.

Практически невероятное (extremely improbable) отказное состояние — отказное состояние, наступление которого не ожидается в течение

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

> эксплуатации всех самолетов данного типа. Его вероятность оценивается как 10^{-9} на час полета или менее.
> Катастрофическое отказное состояние должно быть практически невероятно и не должно возникать в результате какого-либо единичного отказа.

После выхода летной директивы свое мнение о возможных причинах проблемы изложил специалист по информационной безопасности Рубен Сантамарта, на тот момент работавший в компании IOActive и занимавшийся исследованием информационной безопасности самолета Boeing 787. Он предположил, что отказ функции мониторинга мог произойти из-за ошибки в реализации канального уровня передачи данных в специализированной интегральной схеме, используемой в сети CDN.

Ошибки с доставками сообщений в основной бортовой вычислительной сети самолетов Airbus A350

В июне 2017 года Европейское агентство по авиационной безопасности издало директиву летной годности (EASA AD 2017-0129), основанную на сервисном бюллетене компании Airbus. Документ предписывал эксплуатантам самолетов Airbus A350 регулярно (не реже, чем каждые 149 часов) полностью отключать электропитание самолета для предотвращения отказа бортовой вычислительной сети. В директиве указано, что эксплуатанты сообщали о случаях потери связи между системами авионики по основной бортовой вычислительной сети: наблюдались различные отказы — от неполадок резервирующих систем до проблем с отдельными самолетными функциями, реализуемыми с помощью программных приложений на центральном вычислителе. Подробности отказов не приводились.

Анализ, проведенный Airbus, показал, что после 149 часов непрерывной работы систем авионики могла нарушаться доставка сообщений по бортовой вычислительной сети стандарта ARINC 664[16] к программным приложениям на центральных вычислителях. Это могло привести к отказам критичных для безопасности полета систем.

Спустя год после выхода директивы было выпущено обновление программного обеспечения, которое устраняло причину отказа, и опубликован сервисный бюллетень по его установке (Airbus SB A350-42-P010). Еще через год, в июле 2019 года, директива была дополнена (EASA

[16] В самолетах Airbus сети стандарта ARINC 664 называются сетями Aircraft Full Duplex (AFDX).

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

AD 2017-0129R1): для самолетов с обновленным программным обеспечением отключение электропитания больше не требовалось.

Сервисный бюллетень компании Airbus содержит инструкции по обновлению программного обеспечения коммутаторов бортовой вычислительной сети ARINC 664 (Common Remote Data Concentrator, CRDC) и центральных вычислителей (Core Processing Input Output Modules, CPIOM), а также пояснения относительно самой ошибки. После 149 часов непрерывного электроснабжения самолета происходил сброс внутреннего таймера, который встроен в каждое из оконечных устройств сети ARINC 664. Если в этот короткий промежуток времени какое-либо оборудование или система пытались отправить сообщение по сети, то после они не могли отправлять сообщения до полного отключения и повторного включения электропитания самолета.

Стоимость работ по отключению и повторному включению электропитания самолета в директивах Европейского агентства по авиационной безопасности (EASA) не приводилась. В аналогичной директиве летной годности Федерального управления гражданской авиации США (FAA) затраты оценивались по той же методике, что и для самолетов Boeing 787. То есть расходы могли составлять до 5185 долларов в год на один самолет, учитывая только стоимость нормо-часа технического обслуживания. В США на момент публикации директивы было зарегистрировано два самолета Airbus A350. Согласно сервисному бюллетеню, установка программного обеспечения занимала четыре нормо-часа. Время на подготовку, планирование и проверку результата не учитывалось. Компания Airbus брала на себя оплату этих затрат по внутренней ставке гарантийных работ при соблюдении определенных условий.

Особенность этой ошибки заключается в том, что она была выявлена после сообщений эксплуатантов об отказах, притом что она могла привести к катастрофическим отказным состояниям. Несмотря на это прямой ущерб для авиакомпаний-эксплуатантов в результате этой ошибки был незначительный. В контексте кибербезопасности примечательно, что на разработку обновления для устранения ошибки ушло около года.

Ошибка в бортовых регистраторах данных самолетов типа Boeing 787

Проблемы с некорректными метками времени сообщений в бортовых сетях стандарта ARINC 664 напоминают еще об одной проблеме в авионике самолета Boeing 787, которая была выявлена в ходе

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

расследования инцидента с возгоранием литий-ионных аккумуляторных батарей в 2013 году.

У самолета Boeing 787 авиакомпании Japan Airlines в международном аэропорту Логан в Бостоне (Массачусетс, США) вскоре после высадки пассажиров загорелась аккумуляторная батарея. В отчете об инциденте указано, что на начальном этапе расследования возникли сложности из-за проблем с анализом данных бортовых параметрических самописцев (Enhanced Airborne Flight Recorders, EAFR). Оказалось, что после того, как источник прекращал передачу параметрических данных, регистраторы продолжали записывать находящиеся в буфере уже устаревшие данные (stale data) как актуальные. Было отмечено, что использование устаревших данных из регистраторов для оценки технического состояния и проведения технического обслуживания и ремонта самолета могло приводить к нарушению летной годности. В этой связи Национальный совет по безопасности на транспорте США (National Transportation Safety Board, NTSB) рекомендовал Федеральному управлению гражданской авиации США (FAA) и компании Boeing принять определенные меры.

Современные комплексы бортового оборудования накапливают и передают операционным службам авиакомпаний-эксплуатантов большие объемы данных о работе и состоянии различных систем самолета. Эти данные используются для диагностики состояния, технического обслуживания и ремонта как конкретных самолетов, так и всего флота авиакомпании, в том числе для предиктивного обслуживания.

О прямом ущербе для авиакомпаний-эксплуатантов из-за этой ошибки в регистраторах и связанных с ней нарушений безопасности полетов не указывалось. Тем не менее, нарушение целостности собранных данных в результате ошибок и атак на системы авионики может привести к серьезным последствиям, и это нужно учитывать при оценке рисков кибербезопасности.

Существующие подходы к сертификации кибербезопасности цифровых авиационных систем

С 2014 года в США и Евросоюзе публикуется серия стандартов по защите авиационной техники от кибератак для обеспечения и поддержания летной годности. В настоящее время на основе этих стандартов рабочая группа «Авиационного регистра Российской Федерации» (Авиарегистр России)

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

готовит отечественные нормативно-методические документы по обеспечению информационной безопасности (кибербезопасности) авиационной техники. В рабочую группу входят представители ведущих предприятий отечественной авиационной промышленности, таких как «Яковлев», Национальный центр вертолетостроения имени М. Л. Миля и Н. И. Камова, Авиационный комплекс имени С. В. Ильюшина, Уральский завод гражданской авиации, «Лаборатория безопасных систем» (Advalange), Государственный научно-исследовательский институт авиационных систем, а также представители «Лаборатории Касперского».

Наличие стандартов по защите авиационной техники от кибератак для обеспечения и поддержания летной годности свидетельствует о том, что в мировой практике сложился определенный подход в этой области. В этой части статьи мы рассмотрим летную годность с точки зрения ее подверженности кибератакам, определим список целей кибербезопасности авиационной техники и проведем обзор основных нормативно-методических документов (стандартов, руководств и пр.), которые применяются в мировой практике при разработке и эксплуатации авиационной техники.

Примечание 5. Безопасность

В этой статье термин «**безопасность**», когда он используется без каких-либо уточнений, означает отсутствие недопустимого риска нанесения вреда жизни и здоровью людей, имуществу или окружающей среде (согласно определению в ГОСТ Р 57149-2016 (ISO/IEC Guide 51:2014) «Аспекты безопасности. Руководящие указания по включению их в стандарты»).

Летная годность (пригодность для выполнения полетов) — это техническое состояние самолета, при котором самолет соответствует типовой (утвержденной) конструкции и обеспечивается его безопасная эксплуатация.
Безопасность полетов — состояние гражданской авиации или ее отдельных элементов, при котором обеспечивается безопасная эксплуатация самолетов.

Основные цели при обеспечении кибербезопасности систем авионики для самолетов гражданской авиации это:

- защита летной годности (защита технического состояния самолета, установленного нормами летной годности);
- защита безопасности полетов;
- защита технического состояния самолета, установленного требованиями авиакомпании (помимо норм летной годности);

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- защита деловой активности авиакомпании.

Защита летной годности и безопасности полетов — приоритетные цели, так как они связаны с риском для жизни и здоровья людей, а также для окружающей среды.

Рассмотрим каждую цель подробно и представим краткий обзор соответствующих нормативно-методических документов. Некоторыми из этих документов пользуются ведущие зарубежные разработчики авиационной техники и авиационные регуляторы США и Евросоюза. Американские и европейские нормативно-методические документы по кибербезопасности авиационной техники во многом основаны на стандартах информационной безопасности систем общего назначения, в частности на стандартах Международной организации по стандартизации (International Organization for Standardization, ISO), Международной электротехнической комиссии (International Electrotechnical Commission, IEC) и Национального института стандартов и технологий США (National Institute of Standards and Technology, NIST). Основные нормативно-методические документы по кибербезопасности, применяемые в США и Евросоюзе при разработке и эксплуатации самолетов, мы приводим Приложении А.

Защита летной годности

Национальные регулирующие органы, такие как Авиарегистр России, Федеральное управление гражданской авиации США (FAA) и Европейское агентство авиационной безопасности (EASA), предъявляют требования по защите летной годности от кибератак. Эти требования включаются в сертификационный базис самолета[17].

Защита летной годности включает мероприятия по проектированию и реализации средств защиты на этапе разработки (в ходе обеспечения летной годности), а также мероприятия по защите на этапе эксплуатации (в ходе поддержания летной годности).

Раньше критически важные для безопасности полета бортовые системы и сети передачи данных были либо физически изолированы от внешней среды и друг от друга, либо обладали ограниченной и контролируемой связностью. В современных цифровых комплексах бортового

[17] Сертификационный базис — документ, содержащий требования к летной годности и охране окружающей среды, применимые к данному образцу авиационной техники.
Источник: Федеральные авиационные правила «Сертификация авиационной техники, организаций разработчиков и изготовителей авиационной техники. Часть 21». Министерство транспорта Российской Федерации, 2014.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

оборудования на основе IP-сетей передачи данных эти системы могут быть связаны (напрямую или опосредованно) с внешними системами и сетями передачи данных, а также с системами в пассажирском салоне. Возникающие при этом связность и открытость комплексов бортового оборудования регуляторы относят к новым и необычным особенностям конструкции (design features), влияющим на летную годность. Такие конструктивные особенности могут приводить к возникновению новых угроз для летной годности и безопасности полета.

Основной документ, регламентирующий вопросы сертификации воздушных судов, – нормы летной годности. Он содержит набор типовых требований к воздушному судну, соответствие которым обязательно для выдачи сертификата типа воздушного судна. Иногда в ходе сертификации к воздушному судну, помимо требований норм летной годности, регулятором (сертифицирующим органом) предъявляются дополнительные требования. Это может быть вызвано, например, необходимостью сделать исключение из требований норм летной годности или отсутствием в документе требований, регламентирующих особенности конструкции, влияющие на летную годность. Такие дополнительные требования оформляются как специальные технические условия (СТУ). Эти условия являются частью сертификационного базиса воздушного судна наряду с требованиями норм летной годности и указываются в его сертификате типа.

Наличие положений по кибербезопасности в нормах летной годности обязывает сертифицирующий орган учитывать вопросы кибербезопасности вне зависимости от того, считаются ли вводимые в состав воздушного судна цифровые системы новыми и необычными особенностями конструкции, а также устанавливает типовые формулировки соответствующих требований.

Американские нормы летной годности, которые разрабатываются Федеральным управлением гражданской авиации США (FAA), пока еще не содержат требований по кибербезопасности. Поэтому при сертификации типа самолетов с передовыми бортовыми инженерными системами регулятор устанавливает СТУ по кибербезопасности. До июля 2020 года европейские нормы летной годности тоже не содержали требований по кибербезопасности, и в сертификатах типа, выданных Европейским агентством авиационной безопасности (EASA) ранее, также указывались СТУ по кибербезопасности. Действующие в Российской Федерации нормы летной годности пока также не содержат требований по кибербезопасности.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Многие действующие сертификаты типа на современные самолеты, выданные в США и Евросоюзе, содержат СТУ по информационной безопасности. Такие условия указаны, например, в сертификатах типа на следующие самолеты:

- Boeing 787 (версия от 31 января 2025 года);
- Boeing 737 MAX (версия от 28 января 2025 года);
- Airbus A350 (версия 31 от 10 апреля 2025 года);
- Airbus A320 (версия 86 от 4 апреля 2025 года).

Примеры специальных технических условий для самолета Boeing 737 приведены в приложении Б.

Специальные технические условия, как правило, требуют проведения анализа угроз кибербезопасности и связанных с ними рисков для безопасной эксплуатации самолета. Требования к информационной безопасности в сертификатах типов, выдаваемых регуляторами в США и Евросоюзе, практически идентичны. Их можно разделить на три группы:

- требования по защите бортовых систем и сетей от несанкционированного доступа со стороны удаленных или локальных по отношению к этим системам и сетям субъектов;
- требования по анализу угроз кибербезопасности, действующих в процессе эксплуатации бортовых систем и сетей самолета, в том числе угроз, связанных с техническим обслуживанием и ремонтом, а также требования к управлению рисками кибербезопасности;
- требования по созданию руководств для эксплуатантов самолетов по обеспечению кибербезопасности бортовых систем и сетей с целью поддержания летной годности.

Первым самолетом, получившим сертификат типа с СТУ по кибербезопасности, был Boeing 787. Федеральное управление гражданской авиации США (FAA) выдало сертификат в августе 2011 года, а уже в сентябре началась коммерческая эксплуатация самолета.

На момент сертификации Boeing 787 не существовало каких-либо требований или рекомендаций относительно методов подтверждения выполнения СТУ по кибербезопасности. Для этого Федеральное управление гражданской авиации США (FAA) выпустило инструкции и определило критерии с учетом особенностей архитектуры и конструкции комплекса бортового оборудования самолета.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Впоследствии ведущие зарубежные отраслевые организации RTCA (США) и EUROCAE (ЕС)[18] совместно разработали серию стандартов по обеспечению кибербезопасности авиационной техники для защиты летной годности. Эти стандарты издаются в США и Евросоюзе под разными индексами. Например, первый стандарт вышел в 2010 году в Евросоюзе под индексом EUROCAE ED-202, а затем — в США под индексом RTCA DO-326 и часто упоминается как ED-202/DO-326. Для обозначения других стандартов из этой серии используются подобные составные индексы. В ED-202/DO-326 были перечислены меры по кибербезопасности при проектировании и модификации авиационной техники. Позже появился стандарт ED-203/DO-356 с рекомендациями по реализации мер, описанных в первом стандарте. В 2014 году вышел ED-204/DO-355, дополнивший предыдущие стандарты рекомендациями по обеспечению информационной безопасности для поддержания летной годности. А в 2015 году был опубликован стандарт ED-201, определивший общий контекст для всей этой серии.

В настоящее время действуют обновленные версии стандартов: ED-202A/DO-326A (вышел в 2014 году), ED-203A/DO-356A (2018), ED-204A/DO-355A (2020), ED-201A/DO-391 (2021). При сертификации самолета регуляторы США и Евросоюза принимают подтверждение соответствия этим стандартам как доказательство выполнения СТУ по кибербезопасности. Так, в комментарии к СТУ в сертификате типа самолета Boeing 737, выданном Европейским агентством авиационной безопасности (EASA), рекомендуется проводить оценку рисков информационной безопасности в соответствии со стандартом ED-202A/DO-326A.

В июле 2020 года в нормы летной годности Евросоюза было внесено требование по защите бортовых систем от кибератак на основе управления рисками информационной безопасности[19]. В качестве доказательства соответствия нормам принимается подтверждение следования стандартам ED-202A, ED-203A, ED-204A (DO-326A, DO-356A, DO-355A).

[18] RTCA — некоммерческая организация в США, занимающаяся разработкой технических руководств и стандартов в сотрудничестве с регулирующими органами власти из разных стран. EUROCAE (European Organization for Civil Aviation Equipment) — Европейская организация по оборудованию гражданской авиации, занимающаяся стандартизацией как бортовых, так и систем и оборудования.

[19] См. раздел CS 25.1319 в дополнении 25 к нормам летной годности ЕС (Easy Access Rules for Large Aeroplanes (CS-25) (Amendment 25), European Union Aviation Safety Agency (EASA), EASA eRules, June 24, 2020.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Помимо этих стандартов, для соответствия требованиям информационной безопасности применяются стандарты ARINC[20], которые содержат технические спецификации на бортовое электрическое и электронное оборудование, а также протоколы передачи. Эти стандарты разработаны при участии ведущих мировых производителей и эксплуатантов авиационной техники. Стандарт ARINC 664 (ARINC Specification 664 Aircraft Data Network) содержит техническую спецификацию бортовой IP-сети передачи данных, а также рекомендации по техническим мерам защиты.

Для защиты летной годности требуется исключить в случае компрометации дополнительных систем (таких, как электронные планшеты летчиков) их возможное негативное влияние на основные системы. Это требование есть в нормах летной годности или соответствующих СТУ по кибербезопасности. Для некоторых дополнительных систем Федеральное управление гражданской авиации США (FAA) выпустило специальные директивы, в частности руководства по использованию электронной документации и электронных планшетов летчиков. Похожие руководства подготовило и Управление безопасности гражданской авиации Австралии (CASA).

Защита безопасности полетов

Безопасность полетов достигается за счет применения различных мер, среди которых мероприятия по обеспечению и поддержанию летной годности, организации воздушного движения, предоставлению актуальной информации экипажам (планов полетов, электронных карт и схем, данных о метеорологической обстановке, сведений о пассажирах и грузах) и техникам (сведений о конфигурации, состоянии и отказах систем, руководств по технической эксплуатации). Таким образом, помимо защиты непосредственно летной годности, для обеспечения безопасности полетов нужна еще и защита различных эксплуатационных процессов и процедур.

Обеспечение безопасности полетов предполагает взаимодействие бортовых и внешних систем, в том числе в автоматическом режиме. Например, современные технологии организации воздушного движения, такие как технология наблюдения за воздушной обстановкой ADS-B[21],

[20] Организация Aeronautical Radio, Incorporated (ARINC) была основана в 1929 году и сейчас является подразделением компании Collins Aerospace. ARINC публикует технические стандарты и спецификации в области авиационной техники, которые разрабатываются Комитетом авиакомпаний по электронному оборудованию (Airlines Electronic Engineering Committee, AEEC). В состав комитета входят представители ведущих производителей и эксплуатантов авиационной техники.
[21] См. статью New Air Traffic Surveillance Technology, Quarter 2 (QTR_02 10), pp. 7–13.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

задействуют бортовые, наземные и спутниковые системы. В США разрабатывается система организации воздушного движения следующего поколения (Next Generation Air Transportation System, NextGen). В 2015 году Счетная палата США представила Конгрессу доклад о необходимости комплексного подхода к обеспечению информационной безопасности системы NextGen, в котором указывалось на необходимость защиты систем авионики ввиду их высокой связности с внешними системами. В 2020 году Счетная палата США выпустила еще один доклад, в котором рассматривались риски кибербезопасности, связанные с бортовыми системами связи, позиционирования и получения метеоданных. В обоих документах отмечалось, что регуляторам следует улучшить подход к оценке защищенности бортовых систем.

В настоящее время отсутствуют специализированные стандарты по защите безопасности полетов. Тема безопасности полетов затрагивается в стандарте ED-201A/DO-391, который описывает контекст для оценки рисков кибербезопасности в гражданской авиации. В этом стандарте отрасль рассматривается как структура различных взаимодействующих друг с другом сторон (stakeholder framework) с разделением между ними ответственности (responsibility sharing) за обеспечение кибербезопасности.

В США и Евросоюзе при разработке мер защиты в этой области применяются подходящие стандарты и руководства Национального института стандартов и технологий США, например, NIST SP 800-30 и NIST SP 800-53, а также международные стандарты ISO/IEC серии 27000.

Защита технического состояния самолета, установленного требованиями авиакомпании

Нормы летной годности устанавливаются регулирующими органами для обеспечения безопасной эксплуатации самолета. Однако авиакомпании могут иметь свои дополнительные требования к техническому состоянию самолетов. Эти требования касаются, как правило, таких бортовых систем, как информационно-развлекательная система, бортовая информационная система и электронные планшеты летчиков. Стабильная работа этих систем важна для эффективной коммерческой эксплуатации.

Дополнительные требования к техническому состоянию самолета определяются авиакомпаниями с учетом экономической модели перевозок, поддерживаемого уровня сервиса и других факторов. Защиту технического состояния самолета авиакомпании тоже осуществляют сами. Стоит уточнить, что все вопросы, связанные с возможным

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

использованием дополнительных систем для кибератак на основные системы рассматриваются в контексте защиты летной годности. То есть, например, возможное негативное влияние информационно-развлекательной системы на летную годность в случае компрометации системы относится к защите летной годности, а обеспечение ее стабильной работы — к защите технического состояния самолета в соответствии с требованиями авиакомпании.

При защите технического состояния самолета в соответствии с требованиями авиакомпании, как правило, руководствуются стандартами и нормативно-методическими документами по кибербезопасности систем общего назначения, так как авиационные стандарты и руководства в этой области отсутствуют.

Защита деловых интересов авиакомпаний

В условиях рыночной экономики вопросы защиты деловых интересов актуальны как для отдельных участников отрасли — авиакомпаний, производителей авиационной техники, пассажиров, поставщиков товаров и услуг авиакомпаний, так и для отрасли в целом.

Защита деловых интересов подразумевает предотвращение финансовых потерь и защиту репутации. Кибербезопасность всех участников отрасли тесно связана с интересами авиакомпаний и должна находить место в договорных обязательствах и соответствующих нормативных правовых актах. Так, проблема с приложениями для ЭПЛ вроде той, которая привела к задержке рейса авиакомпании American Airlines, должна иметь последствия для разработчика (поставщика) этого решения. А чтобы избежать подобных проблем на системном уровне, требования к приложениям должны формироваться в отрасли, а не только в частных технических заданиях на разработку. Это касается не только ЭПЛ, но и всех дополнительных систем КБО, а также внешних систем вплоть до систем бронирования авиабилетов.

Авиационные регуляторы занимаются только вопросами, связанными с летной годностью и безопасностью полетов, — защита интересов участников отрасли вне сферы их деятельности. По этой причине в авиационных стандартах по кибербезопасности этот аспект защиты не учитывается. Исключение — стандарт ARINC 811, в котором кибербезопасность самолета рассматривается в контексте его коммерческой эксплуатации авиакомпанией. Этот стандарт содержит рекомендации по структуре процесса обеспечения кибербезопасности самолета для авиакомпаний с учетом их деловых интересов. Также, как и

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

для защиты технического состояния самолета, применяются стандарты для систем общего назначения.

Заключение

Обзор некоторых инцидентов, вызванных сбоями в программно-аппаратном обеспечении комплексов бортового оборудования современных самолетов гражданской авиации, показывает необходимость анализа рисков кибербезопасности и обоснования должной защиты от кибератак, которые могут вызвать подобные сбои.

Рассмотренные примеры авиационных событий показывают, что ошибки и сбои в работе программного обеспечения систем КБО могут привести как к незначительному нарушению операционной деятельности авиакомпании, так и к катастрофам. В авиации за безопасность полетов и поддержание должного технического состояния самолетов отвечают многие участники отрасли, каждый из которых при этом защищает собственные деловые интересы. Возрастающая связность и открытость систем КБО в ходе их цифровизации и интеграции с внешними системами делает кибератаки вероятными, а ущерб — возможным.

Существующие специальные подходы к оценке защищенности цифровых систем КБО, используемые при сертификации самолетов, ограничены проверками выполнения требований по защите авиационной техники от кибератак для обеспечения и поддержания летной годности. Эти требования касаются только технического состояния самолета и не рассматривают безопасность полетов в комплексе.

В то же время требования по защите безопасности полетов от кибератак имеют более общий характер, так как относятся ко всему комплексу различных систем и технологий, задействованных в организации воздушного движения. Эта область является ближайшей в исследовании и стандартизации требований кибербезопасности авиационных систем.

Правила защиты технического состояния самолета для обеспечения эффективной коммерческой эксплуатации и защита от кибератак авиакомпаний, производителей авиационной техники, поставщиков товаров и услуг авиакомпаний, а также пассажиров сейчас не рассматриваются на уровне отраслевых рекомендаций и стандартов. Универсальных стандартов по управлению кибербезопасностью и оценке рисков, дополненных внутренними руководствами, пока достаточно. Однако в ходе дальнейшей интеграции систем и усложнения информационной инфраструктуры гражданской авиации, возможно, будут

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

появляться специализированные стандарты и руководства, касающиеся рисков кибербезопасности в конкретных сценариях (например, регламентирующие использование цифровых двойников или систем искусственного интеллекта).

Приложение А. Перечень зарубежных стандартов и директив в области информационной безопасности самолетов гражданской авиации

Европейский стандарт ED-201: Aeronautical Information System Security (AISS) Framework Guidance определяет общий контекст защиты бортовых систем.

При проектировании и производстве самолетов для достижения соответствия нормам летной годности и получения сертификата типа в США и Евросоюзе используются следующие стандарты:

- европейский стандарт ED-202A: Airworthiness Security Process Specification и его американский аналог DO-326A, которые содержат основные положения по обеспечению информационной безопасности воздушного судна и его систем;
- европейский стандарт ED-203A: Airworthiness Security Methods and Considerations и американский аналог DO-356A, которые содержат рекомендации по реализации положений ED-202A/DO-326A.

Для поддержания летной годности в ходе эксплуатации используются следующие стандарты и директивы (циркуляры):

- европейский стандарт ED-204A: Airworthiness Security Process Specification и его американский аналог DO-355A;
- европейский стандарт ED-206A: Guidance for Security Event Management и его американский аналог DO-392;
- директива FAA по обеспечению информационной безопасности бортовых сетей передачи данных для поддержания летной годности AC 119-1: Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP);
- директива FAA по использованию электронных подписей и ведению электронных журналов и руководств AC 120-78B: Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals;

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- директива FAA по допуску к эксплуатации электронных планшетов летчиков (ЭПЛ) AC 120-76E: Authorization for Use of Electronic Flight Bags;
- директива FAA по работе с программным обеспечением в ходе технического обслуживания и ремонта воздушных судов AC 43-216A: Software Management During Aircraft Maintenance.

Помимо перечисленных документов, для обеспечения соответствия требованиям специальных технических условий по информационной безопасности используются стандарты ARINC. При разработке бортовых сетей передачи данных на основе протокола IP (IP-сетей) применяется стандарт ARINC Specification 664: Aircraft Data Network, одна из частей которого, ARINC Specification 664P5, содержит рекомендации по выделению логических сетевых доменов и положения по обеспечению информационной безопасности в бортовых сетях передачи данных. В некоторых стандартах ARINC приводятся рекомендации по конкретным техническим мерам для обеспечения и поддержания летной годности:

- ARINC Report 852: Guidance for Security Event Logging in an IP Environment;
- ARINC Report 835-1: Guidance for Security of Loadable Software Parts Using Digital Signatures;
- ARINC Report 842-1: Guidance for Usage of Digital Certificates.

Стандарт ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework содержит рекомендации для авиакомпаний по обеспечению информационной безопасности самолетов. Он выделяется из других документов тем, что в нем прямо или косвенно учитываются все четыре цели информационной безопасности самолета.

Если для доказательства соответствия СТУ используется какой-либо стандарт, то он становится частью практических руководств (инструкций) по поддержанию летной годности самолета.

Приложение Б. Специальные технические условия по информационной безопасности в зарубежных сертификатах типа на самолет Boeing 737

Предлагаем переводы специальных технических условий по информационной безопасности, которые указаны в сертификатах типа на

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

самолет Boeing 737 модификации Next Generation (-600/-700/-700C/-800/-900/-900ER) и MAX (8/9/-8200), выданных Федеральным управлением гражданской авиации США (FAA) и Европейским агентством по авиационной безопасности (EASA).

Специальные технические условия по информационной безопасности в сертификате типа FAA

В сертификате типа A16WE от 15.03.2023 (версия 73), выданном Федеральным управлением гражданской авиации США (FAA), указаны два специальных технических условия по информационной безопасности:

25-550-SC «Защита электронных систем самолета от неавторизованного (несанкционированного) доступа со стороны внешних источников»:

1. Заявитель обязан защитить электронные системы самолета от доступа из внешних неавторизованных источников, включая возможные вмешательства в ходе технического обслуживания и ремонта.

2. Заявитель обязан выявить и оценить угрозы и реализовать меры информационной безопасности для электронных систем с целью защиты самолета от любого негативного влияния на безопасность, функциональность и летную годность.

3. Заявитель должен разработать процедуры, позволяющие эксплуатанту поддерживать летную годность самолета, в том числе при внесении в сертифицированную конструкцию изменений, которые могут негативно повлиять на работу утвержденных мер обеспечения информационной безопасности электронных систем.

25-551-SC «Изоляция или защита электронных систем самолета от неавторизованного доступа со стороны внутренних источников»:

1. Заявитель обязан реализовать в конструкции самолета изоляцию или защиту электронных систем от доступа из внутренних неавторизованных источников. Конструкция должна исключать возможность случайных и преднамеренных изменений, а также любые негативные воздействия на оборудование, системы, сети и другие компоненты, необходимые для безопасного полета и безопасной эксплуатации.

2. Заявитель должен разработать процедуры, позволяющие эксплуатанту поддерживать летную годность самолета, в том числе при внесении в сертифицированную конструкцию изменений, которые могут негативно повлиять на работу утвержденных мер обеспечения информационной безопасности электронных систем.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Специальные технические условия по информационной безопасности в сертификате типа EASA

В сертификате типа IM.A.120 от 10.01.2023, выданном Европейским агентством по авиационной безопасности (EASA), указано одно специальное техническое условие по обеспечению кибербезопасности вычислительных систем и сетей, которое фактически является набором из трех условий:

a) заявитель должен обеспечить защиту систем и сетей самолета от доступа из внешних или внутренних неавторизованных источников, если повреждение этих систем и сетей, включая аппаратное и программное обеспечение, а также данные, вследствие непреднамеренного или преднамеренного неавторизованного воздействия может нарушить безопасность;

b) заявитель должен выявить и оценить угрозы информационной безопасности, в том числе те, которые могут возникнуть в результате технического обслуживания и ремонта, при незащищенном подключении устройств или использовании оборудования, находящегося на борту самолета или вне его. Помимо этого, заявитель должен минимизировать риски, связанные с угрозами информационной безопасности, для защиты систем самолета от любых негативных воздействий на безопасность;

c) должны быть разработаны процедуры для поддержания утвержденного уровня защищенности систем и сетей самолета в случае внесения изменений в сертифицированную конструкцию.

В сертификате приводятся рекомендации по методам подтверждения соответствия этому СТУ, в том числе по верификации механизмов безопасности.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»