ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БОРТУ ВОЗДУШНОГО СУДНА

Владислав КОСЬЯНЧУК, заместитель генерального директора ФГУП «ГосНИИАС», доктор технических наук, профессор РАН;
Николай СЕЛЬВЕСЮК, заместитель генерального директора ФГУП «ГосНИИАС», доктор технических наук, профессор РАН;
Евгений ЗЫБИН, начальник лаборатории ФГУП «ГосНИИАС», доктор технических наук;
Рашит ХАММАТОВ, начальник лаборатории ФГУП «ГосНИИАС», кандидат технических наук;
Сергей КАРПЕНКО, инженер, ФГУП «ГосНИИАС».

В статье проводится анализ тенденций информатизации и интеграции бортового оборудования воздушных судов (ВС). Рассматриваются инциденты и потенциальные уязвимости информационной безопасности на борту воздушного судна. Приведены зарубежные стандарты по обеспечению информационной безопасности в авиации и требования российского законодательства к обеспечению информационной безопасности объектов критической инфраструктуры. Описана концепция обеспечения информационной безопасности на борту воздушного судна как на этапе разработки его бортового оборудования, так и на этапе его эксплуатации.

Введение

В существующих воздушных судах (ВС) используются различные системы передачи данных. К ним относятся: спутниковые навигационные системы GPS и ГЛОНАСС, системы автоматического зависимого наблюдения АЗН-В, системы радионавигации VOR/DME, системы посадки ILS, MLS, система предупреждения столкновений TCAS, система обмена электронными сообщениями ACARS и CPDLC, технология определения местоположения MLAT, автоматический указатель направления ADF, спутниковая и голосовая ВЧ и ОВЧ связь, первичный и вторичный радиолокаторы, радиовысотомер и другие средства обмена информацией.

Для повышения эффективности гражданских перевозок на перспективных ВС должны использоваться технологии и процессы для увеличения пропускной способности и обеспечения безопасности каналов передачи данных. Такие ВС с поддержкой постоянной связи (E-enabled) будут играть ключевую роль в будущем [1, 2].

ВС имеют множество каналов передачи данных для обслуживания различных функций:

- управление движением самолета путем управления

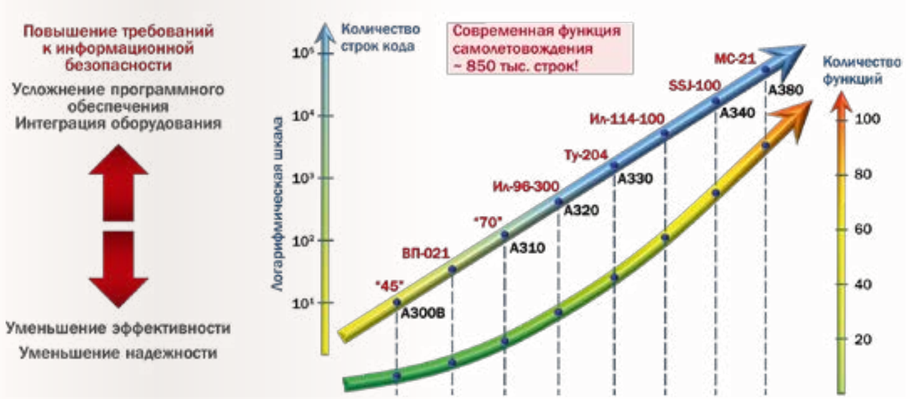


Рис. 1. Тенденции информатизации воздушных судов

аэродинамическими поверхностями и тягой двигателей;

- предоставление навигационной и технической информации экипажу и операционному центру авиакомпании;
- контролирование систем освещения и развлечения;
- передача сообщений, развлечение и информирование пассажиров на борту ВС, связь с аэропортом и т.д.

Все это обеспечивает высокий уровень эффективности воздушных перевозок. Однако, с увеличением количества каналов передачи данных и ростом сложности сетей, в них неизбежно будут возникать уязвимости, которые присущи любой информационной системе.

В данной статье описывается новая концепция построения бортовой информационно-вычислительной сети ВС, позволяющая разделить информационно-вычислительное пространство ВС по уровням доверия с целью обеспечения безопасного обмена данными на борту ВС и за его пределами.

Развитие информационно-вычислительных сетей ВС

Традиционно ВС представляло собой относительно закрытую информационную систему. Все устройства и приборы ВС являлись автономными, без возможности подключения к ним и передачи информации во время полета, благодаря чему обладали высоким уровнем безопасности с точки зрения несанкционированного вмешательства из внешней среды. В результате развития цифровой микроэлектроники, перехода к преимущественно цифровым методам обработки и предоставления данных, увеличения степени информатизации (интеллектуализации) комплекса бортового оборудования (КБО) ВС существенно возросла сложность информационно-вычислительного пространства на его борту (рис. 1) [2–6].

Развитие микроэлектроники и вычислительной техники, их интенсивное проникновение в авиационную электронику обуславливали постоянное развитие и создание качественно новых поколений КБО (рис. 2).

Наиболее старой архитектурой авионики считается независимая архитектура, появившаяся в 1920-х гг. при установке первого радиооборудования на ВС. Частичная автоматизация пилотирования была достигнута в 1950-х гг. путем введения в контур управления простейшего автопилота, осуществлявшего стабилизацию высоты полета и улучшающего управляемость ВС. Тем не менее, доминирующая роль человека в управлении сохранялась, оно по-прежнему велось по отдельным приборам, а бортовой комплекс на данном этапе еще не был сформирован. В

Рис. 2. Развитие архитектуры бортового оборудования воздушных судов

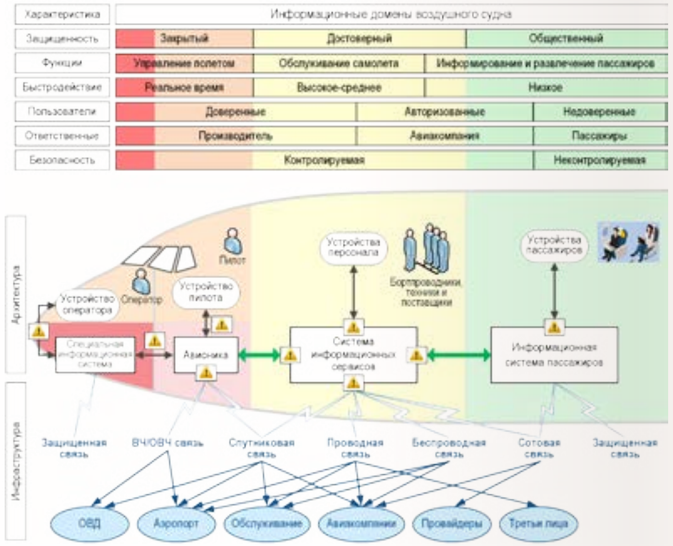


Рис. 3. Информационная архитектура и инфраструктура ВС

данной архитектуре все подсистемы являлись полностью независимыми (автономными), имели свои аналоговые вычислители, датчики, дисплеи и органы управления, за исключением общих источников питания. Полностью независимая архитектура использовалась вплоть до 1970-х годов и сейчас вышла из употребления. Тем не менее, до сих пор в структуре КБО ВС остаются некоторые полностью автономные системы, выполняющие критически важные функции.

Появление первого КБО (централизованная архитектура, 1970-1990 гг.) связано с введением в контур управления специальной вычислительной машины, позволяющей решать задачи траекторного управления ВС. Под КБО стали понимать совокупность управляющей вычислительной машины, приборов и систем, объединенных единой целью управления. Первые КБО ВС имели одну вычислительную машину и были построены по централизованному принципу на базе аналогового вычислителя. Их связи друг с другом были минимальны и представляли собой радиальные соединения «источник-приемник».

В дальнейшем КБО стал строиться по федеративному принципу (федеративная архитектура, 1980-н.в.), предполагающему наличие нескольких отдельных специализированных вычислителей. Его главным отличием являлось независимое распределение функций КБО между отдельными подсистемами. Каждая функция реализовывалась с помощью отдельного аппаратного и программного обеспечения.

С начала 2000-х годов архитектура КБО ВС начала развиваться в соответствии с концепцией интегрированной модульной авионики (ИМА). (Е.Федосов, А.Квочур. «Авионика ближайшей перспективы». «Авиапанорама» №3-2013. –*Прим. ред.*). Под ИМА понимается концепция построения КБО, базирующаяся на открытой сетевой архитектуре и единой вычислительной платформе. Отдельные вычислительные машины со своими интерфейсами, присущие федеративным системам, заменяются общими информационными ресурсами – процессорами, модулями памяти, коммуникационными шинами, интерфейсами ввода-вывода.

Согласно известным публикациям дальнейшее развитие архитектуры КБО ВС не подразумевает революционных изменений по сравнению с концепцией ИМА, а осуществляется по принципу увеличения функциональности. Известны следующие названия разрабатываемых в настоящее время архитектур: ИМА 2-го и 3-го поколений, распределенная ИМА, распределенная электроника, интегрированная распределенная модульная авионика и т.д. Независимо от названия, модернизация архитектуры КБО реализуется путем увеличения количества оборудования, функции которого интегрируются в единый бортовой вычислитель, а также «приближения» единого вычислителя к неинтегрированным системам, датчикам и исполнительным устройствам за счет использования удаленных концентраторов данных (RDC), удаленных контроллеров электроники (RCE), удаленных контроллеров графики и видео (RGVC), удаленных контроллеров питания (RPC) и т.д.

В настоящее время основными направлениями совершенствования КБО является его реализация в виде распределенной структуры и единого информационно-вычислительного пространства, а также создание комплексированных и многофункциональных радиоэлектронных систем, и расширение их взаимодействия с другими системами как на борту, так и на земле [3–5, 7].

Распределенный и интегрированный принципы построения архитектуры КБО ВС на базе открытой сетевой архитектуры и единой вычислительной платформы с использованием бортовых беспроводных сетей, удаленных концентраторов данных, контроллеров электроники,

питания графики и видео обусловили повышение степени внутренней информационной связности БС [5–9]. В результате повышения степени интегрированности с внешними, в т.ч. публичными сетями, КБО ВС стал принимать и отдавать множество различных сигналов во внешний мир, существенно повысив также степень внешней информационной связности ВС (рис. 3).

Для обеспечения эффективного обмена данными на борту ВС и за его пределами информационно-вычислительная система ВС разделяется на информационные домены с разной степенью защищенности:

- домен управления ВС (закрытый);
- домен информационных услуг воздушного судна (достоверный);
- домен бортовой развлекательно-информационной системы (общественный) [10–12].

Домен управления ВС обладает высоким уровнем доверия и включает в себя системы управления полетом, навигационные и радиосистемы, а также другие системы, которые работают в высоконадежной среде интегрированной модульной авионики. Он состоит из двух доменов: домена авионики и домена пилота (оператора). К домену авионики относятся все критически важные системы для надежного управления воздушным судном. Он имеет самый высокий уровень требований безопасности и состоит из систем и сетей, основными функциями которых являются обеспечение безопасной и эффективной эксплуатации ВС. Является наиболее важным, защищенным и детерминированным доменом ВС. Все системы, не входящие в домен авионики, можно объединить в одно информационно-вычислительное пространство, условно называемое внешней средой. Домен пилота (оператора) включает в себя информационно-управляющее поле кабины, с помощью которой экипаж взаимодействует с авионикой ВС. Также он содержит систему управления пассажирским салоном, которая выполняет функции, связанные с эксплуатацией салона ВС (контроль состояния окружающей среды в салоне, информационные обращения к пассажирам, обнаружение дыма и т.п.).

Домен информационных услуг воздушного судна предоставляет информацию для обслуживающего и технического персонала и обеспечивает безопасное соединение между независимыми доменами ВС: авионики, системы развлечения пассажиров и любыми внешними сетями. Включает в себя домен обслуживания ВС, предоставляющий оперативную и административную информацию для экипажа ВС (обслуживающего и технического), а также домен поддержки пассажиров, предоставляющий информацию в информационную систему пассажиров.

Домен бортовой развлекательно-информационной системы предоставляет информацию и развлекательные услуги пассажирам. Домен может содержать несколько систем от разных поставщиков, которые могут быть связаны друг с другом, а его границы не обязательно должны соответствовать границам физических устройств. Помимо традиционных систем развлечений, он может также включать в себя системы подключения к пассажирским устройствам, информационным системам полета, широкополосное телевидение, системы связи и сообщений, а также функции информационного сервера, предоставляющего услуги пассажирам. Включает в себя два домена: домен информационной системы пассажиров и домен пассажирских устройств. Домен информационной системы пассажиров обеспечивает необходимой информацией пассажиров и позволяет им управлять салоном через панель бортпроводников (свет, приводы кресел, система вызова персонала), проводить операции по кредитной карте, пользоваться бортовой беспроводной и сотовой связью, подключать к сети мобильные телефоны, планшеты и ноутбуки. В домен пассажирских устройств включаются только те устройства, которые пассажиры могут пронести на борт. Они могут подключаться к воздушной сети или друг к другу.

Внутренние и внешние связи постоянно возрастают вследствие увеличивающейся пропускной способности сетей передачи данных, объемов памяти, хранения, скорости работы и производительности процессоров с одновременным уменьшением занимаемой площади, массы и стоимости компонентов. Уменьшение веса, стоимости, улучшение интеграции и эксплуатации – одни из преимуществ широкого разделения составных бортовых частей воздушного судна на домены с разной степенью защищенности.

Угрозы информационной безопасности на борту воздушного судна

Угрозы информационной безопасности в нынешних условиях являются неотъемлемой частью деятельности всей авиационно-транспортной системы в мире. Более того, в ряде случаев они стали важнейшими задачами обеспечения гарантированного уровня безопасности полетов наряду с экономической эффективностью деятельности отдельных авиапредприятий и авиакомпаний.

Активное обсуждение вопросов обеспечения информационной безопасности гражданской авиации на проходящих научно-технических конференциях, совещаниях ИКАО свидетельствуют о большой актуальности многих ключевых проблем, связанных с серьезными разрушительными последствиями при нарушении информационной безопасности (ИБ), недостаточной эффективностью средств защиты и т.д.

Развитие информационно-вычислительных сетей ВС привело к возрастанию потенциала уязвимости КБО ВС от деструктивных воздействий нарушителей как случайного, так и преднамеренного характера. Хакеры, вторгающиеся в работу авиационных систем, способны не только добывать циркулирующую в них информацию, но и искажать достоверность информации, например, о воздушной обстановке, параметрах самолетовождения, данных коммерческого характера и т.п., что может негативно сказаться на различных процессах управления и организации воздушного движения.

Новейшие достижения в области компьютерных наук, информационных технологий, средств коммуникации, способствовали не только техническому прогрессу в авиации, но и появлению потенциальных уязвимостей информационной безопасности и новых инцидентов в

Таблица 1. Потенциальные уязвимости информационной безопасности в авиации

Описание уязвимости	Год
Самолет WestJet передал код 7500, что обозначает угон. Возможно, данное сообщение было передано киберпреступником.	2015
Эксперт по вопросам информационной безопасности заявил, что он смог взломать и изменить направление движения воздушного судна в середине полета, вторгнувшись в систему развлечений пассажиров.	2014
Потенциальной уязвимостью в программировании электронных бортовых журналов могут воспользоваться киберпреступники при подключении их к внешним сетям для обновлений.	2012
Хакер продемонстрировал теоретическую возможность использовать Android для удаленной атаки и захвата самолета.	2012
Хакер продемонстрировал уязвимость в управлении воздушным движением. Благодаря недорогим коммерческим аппаратным и программным средствам ему удалось обмануть сигналы АЗН-В так, что на экране диспетчера появился несуществующий самолет.	2012
FAA заявила, что некоторые компьютерные системы Boeing 747-8 и Boeing 747-8F могут быть уязвимы для внешних атак из-за интерфейсов их подключения.	2010
FAA заявила, что архитектура Boeing 787 позволяет создавать новые виды подключений к ранее изолированным сетям передачи данных, которые подключены к системам, выполняющим критически важные операции, необходимые для обеспечения безопасности полета самолета.	2008

Таблица 2. Инциденты информационной безопасности в авиации

Инцидент	Год	Место	Описание
Кибератака компьютерной системы авиакомпании	2015	Польша	Хакеры атаковали компьютерную систему LOT Polish Airlines, заземлив несколько самолетов.
Кибератака через систему развлечений самолета	2015	США	Хакер нашел слабое место в системе развлечения на самолетах Boeing 737-800, 737-900, 757-200 и Airbus A320 и проник в системы авионики.
Кибератака самолета	2014	Южно-Китайское море	Взломана компьютерная система самолета, в результате чего произошел угон самолета Boeing 777-200 авиакомпании Malaysia Airlines рейса MH370.
Подмена цели	2014	Австрия, Германия, Чехия, Словакия	Многие самолеты исчезли с экранов радаров. Возможно, это было вызвано военными учениями.
Кибератака	2013	Турция	Паспортный контроль в Международном аэропорте имени Ататюрка в Стамбуле был закрыт из-за кибератаки.
Кибератака и фишинг	2013	США	Работа 25 аэропортов была нарушена в результате кибератак и фишинга.
Вредоносный код	2011	США	В программном коде произошел срыв работы, из-за чего службы регистрации аэропорта перестали функционировать и задержали значительное количество полетов во многих аэропортах.
Крушение рейса Spanair 5022	2008	Испания	Компьютерная система, отвечающая за мониторинг технических проблем на борту, была заражена хакерской программой.
Взлом электронных бортовых журналов	2007	Таиланд	Вирус был загружен в электронные бортовые журналы Thai Airways и отключил их, также он был распространен на другие электронные журналы.
Возможность совершения кибератаки на системы УВД Аляски	2006	США	Федеральное управление гражданской авиации США закрыло системы УВД на Аляске в качестве меры предосторожности против нападения в Интернете.

авиации (табл.1, 2) [13– 15].

Основными источниками угроз информационной безопасности на борту ВС могут быть:

- недекларированные возможности встроенного и функционального ПО бортового оборудования и АСУ наземных служб;
- уязвимости бортовых и наземных средств связи, навигации, наблюдения и наведения;
- уязвимости бортовых информационно-вычислительных сетей ВС;
- уязвимости бортовых беспроводных и сенсорно-актуаторных сетей ВС.

Вскрытие в используемых технологиях уязвимостей информационной безопасности, способствующих успешным действиям нарушителя, и принятие активных мер защиты по поддержанию устойчивого функционирования авиационных систем и сетей в условиях возможного воздействия нарушителя являются основными задачами при решении проблем обеспечения информационной безопасности.

Стандарты информационной безопасности в авиации

В табл. 3 приведены стандарты по обеспечению информационной безопасности для поддержания летной годности воздушных судов (ARINC 811, ARINC 664, DO-326, DO-326A, DO-356, DO-356A, DO-355, ATA Spec 42 и др.).

Таблица 3. Стандарты информационной безопасности в авиации

Стандарт	Название	Описание
ARINC 811 (2005)	Commercial aircraft information security concepts of operation and process framework	Приведены терминологические основы информационной безопасности бортовых сетей, описан подход к оценке состояния информационной безопасности.
ARINC 664 (2005-2009)	Aircraft data network	Приведены методы построения детерминированной бортовой сети Ethernet. Определены домены информационной безопасности на борту воздушного судна.
ED-202 / DO-326 (2014)	Airworthiness security process specification	Приведены руководящие принципы процесса обеспечения информационной безопасности
ED-202A /DO-326A (2018)		
ED-203 / DO-356 (2014)	Airworthiness security methods and considerations	Приведены методы и инструменты для достижения целей процесса обеспечения безопасности.
ED-203A / DO-356A (2018)		
ED-204 / DO-355 (2014)	Information Security Guidance for Continuing Airworthiness	Приведено руководство по обеспечению информационной безопасности для поддержания летной годности.
ATA Spec 42 (2017)	Aviation industry standards for digital information security	Приведены требования к взаимной идентификации и управлению доступом между отдельными узлами и агрегатами самолета.

В РФ стандарты информационной безопасности в авиации отсутствуют. Однако необходимо отметить вступивший в силу 01.01.2018 г. Федеральный Закон РФ №187 «О безопасности критической компьютерной инфраструктуры Российской Федерации», и вступившее в силу 21.02.2018 г. Постановление Правительства РФ «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

В соответствии с данными законными актами информационно-вычислительная система любого ВС является объектом критической информационной инфраструктуры (КИИ) РФ, так как попадает под определение автоматизированной системы управления, функционирующей в сфере транспорта. При этом в зависимости от вместимости и маршрутов полетов разные ВС могут иметь различные категории значимости (табл. 4).

Согласно требованиям данных актов, все значимые объекты КИИ РФ должны быть оборудованы программными и программно-аппаратными средствами защиты, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Обеспечение информационной безопасности на этапе разработки

Таблица 4. Показатели и критерии социальной значимости объектов критической информационной инфраструктуры РФ

Показатель	Значение показателя		
	III категория	II категория	I категория
Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые по количеству людей, для которых могут быть недоступны транспортные услуги (человек)	более или равно 50, но менее 1000	более или равно 1000, но менее или равно 5000	более 5000

Обеспечение ИБ современных и перспективных ВС осуществляется как на этапе их разработки, так и на этапе эксплуатации. Обеспечение ИБ на этапе разработки осуществляется за счет совершенствования технологической чистоты процессов проектирования в соответствии с постоянным усложнением авиационной техники и соответствующим развитием нормативной базы (Р-4754→Р-4754А, Р-4761→Р-4761А, КТ-178А→КТ-178В→ КТ-178С и т.д.). Процесс обеспечения ИБ на этапе разработки ВС состоит из трех взаимосвязанных процедур: разработки требований ИБ, разработки ПО и аппаратуры, интеграции и испытаний (рис. 4).

Разработка детальных требований ИБ представляет собой нисходящий процесс проектирования КБО, так как распределение требований производится от самого верхнего уровня (требования к самолету) до самого нижнего детального уровня (требования к ПО и аппаратуре). Для удовлетворения всех требований осуществляется предварительная оценка ИБ самолета и его систем, анализируются потенциальные угрозы ИБ до уровня ПО и аппаратуры, а также возможные источники их возникновения. Это позволяет связать воедино все уровни требований ИБ – самолета, систем, ПО и аппаратуры.

Для автоматизации процесса разработки КБО разрабатываются инструментальные средства поддержки жизненного цикла создания системного и прикладного ПО, включающие: безопасный компилятор с языка Си (гарантия использования только безопасных оптимизаций, сохранение структуры кода для точного анализа тестового покрытия), средства статического и динамического

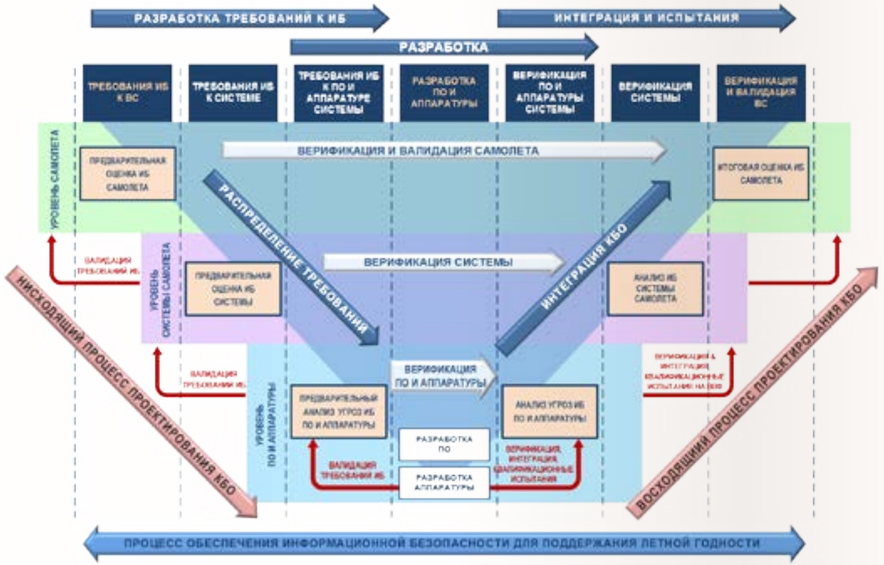


Рис. 4. Обеспечение информационной безопасности на этапе разработки

анализа, средства дедуктивной верификации Си-программ, формальную инспекцию, модульное и интеграционное тестирование, анализ покрытия и характеристик кода и др. Используемые языки, методы и инструменты формальной спецификации и верификации модели политик ИБ отвечают всем критериям оценки безопасности информационных технологий в соответствии с ГОСТ ИСО/МЭК 15408 [16–18].

Обеспечение информационной безопасности на этапе эксплуатации

Обеспечение безопасной и эффективной интеграции бортовых, воздушных и наземных сетей осуществляется за счет разделения информационно-вычислительного пространства ВС по уровням доверия на безопасные контролируемые домены и внедрения между ними дополнительных средств защиты (рис. 5)[1]:

- бортового защищенного шлюза;
- бортовых защищенных серверов.

С помощью группирования бортового оборудования на безопасные домены четко устанавливаются границы, внутри которых обмен информацией должен отвечать наивысшим требованиям безопасности, в то время как другие домены могут иметь более низкий уровень доверия и тем самым взаимодействовать с сетями общего пользования, не беспокоясь о том, что потенциальные угрозы могут навредить жизненно важным системам ВС.

В процессе обеспечения информационной безопасности данные устройства, непрерывно получая пакеты данных из сети, производят выборку и извлечение необходимых характеристик трафика для передачи их интеллектуальному алгоритму обнаружения угроз информационной безопасности, который определяет, являются ли анализируемые данные безопасными. Общей целью бортовой системы обеспечения информационной безопасности является подтверждение того, что риски реализации всех угроз информационной безопасности на борту ВС через все возможные сценарии имеют допустимый уровень.

А. Бортовой защищенный шлюз

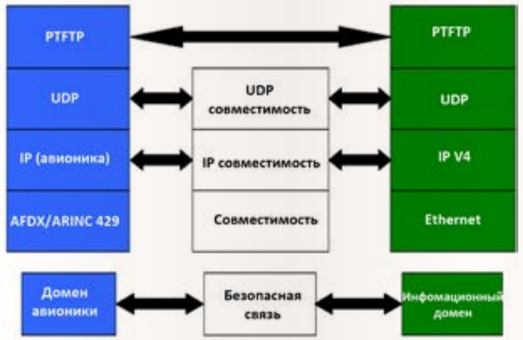
Бортовой защищенный шлюз представляет из себя межсетевой экран, осуществляющий контроль сетевого трафика и обеспечивающий защищенную связь между доменом авионики и внешней средой.

Функциями бортового защищенного шлюза являются:

1) трансляция протоколов домена авионики и информационного домена;
2) инспекция состояния информационной безопасности;
3) безопасная управляемая коммутация.

Для трансляции протоколов, позволяющей скрыть

Рис. 6. Трансляция протоколов в бортовом защищенном шлюзе



1 http://www.ashleyproject.eu

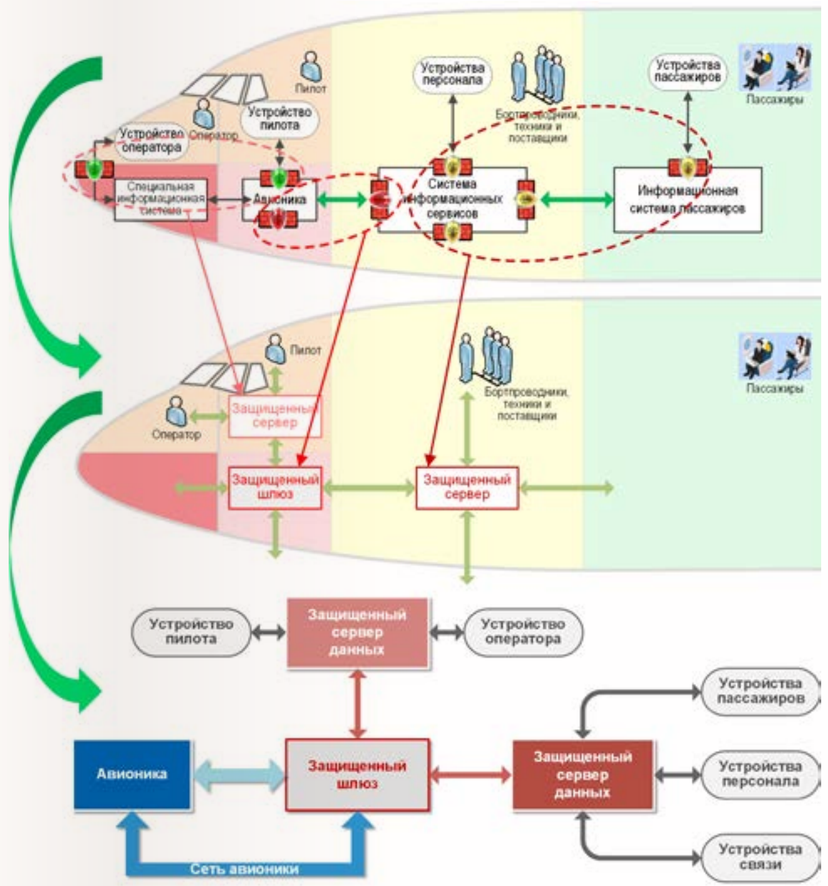


Рис. 5. Архитектура информационной безопасности воздушного судна

Рис. 7. Принцип работы бортового защищенного шлюза

топологию сети от злоумышленника, в шлюзе используются заголовки всех транслируемых протоколов (рис. 6).

Инспекция состояния информационной безопасности осуществляется за счет (рис. 7):

- безопасной маршрутизации;

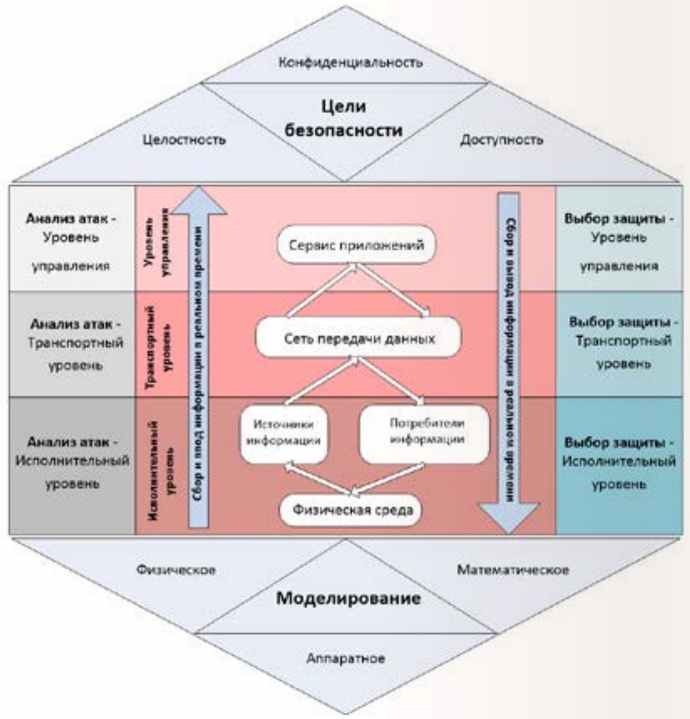
Рис. 8. Состав и принцип работы бортового защищенного сервера

- фильтрации трафика из не доверенных доменов;
- использованием посредников прикладного уровня;
- регистрации событий информационной безопасности.

В защищенном шлюзе реализованы также различные наборы прокси-серверов и служб аутентификации, которые позволяют фильтровать входящие потоки данных из внешней среды, предназначенные для авионики. Работа шлюза, как и всех межсетевых экранов, основана на использовании информации разных уровней модели OSI, на которых системы взаимодействуют друг с другом – начиная с уровня физической среды передачи данных и заканчивая уровнем прикладных программ, используемых для коммуникаций. В общем случае, чем выше уровень модели OSI, на котором шлюз фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты. Такой подход позволяет выделить наиболее критические системы ВС в отдельный домен, доступ к которому будет предоставлен только конкретным пользователям через бортовой защищенный шлюз, без возможности вмешательства сторонних устройств.

В шлюзе осуществляется регистрация событий, имеющих отношение к информационной безопасности ВС. К таким событиям относятся пропуск или блокирование

Рис. 9. Функциональная архитектура бортового защищенного сервера



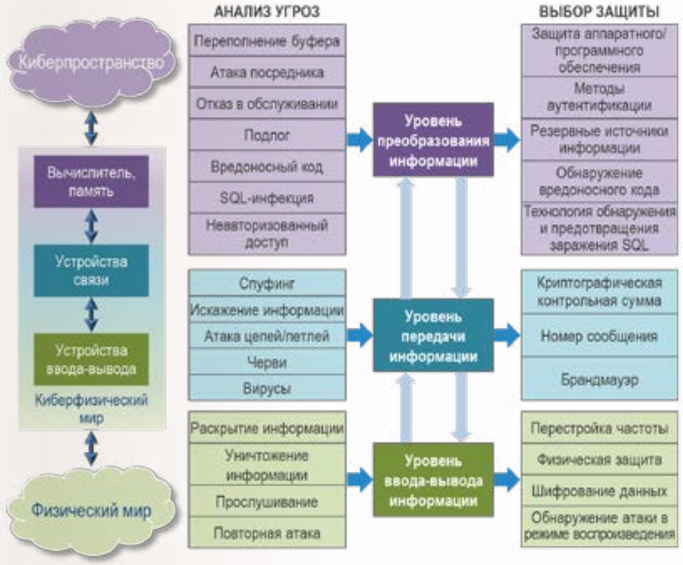


Рис. 10. Принцип работы бортового защищенного сервера

сетевых пакетов, изменение правил разграничения доступа и другие действия.

Б. Бортовой защищенный сервер

Бортовой защищенный сервер представляет собой интеллектуальное защищенное устройство связи, обеспечивающее хранение всей информации из внешней среды, доступ к которой может получить каждый из доменов. Он получает всю необходимую информацию о полете и техническом состоянии ВС и управляет двунаправленным потоком данных между авионикой и внешней средой [19].

В состав бортового защищенного сервера входят (рис. 8):

- защищенный коммуникационный модуль;
- сервер информации;
- серверы приложений.

Функции бортового защищенного сервера (рис. 9):

1. Хранение потенциально недостоверной информации, доступ к которой может получить любой из доменов.
2. Управление двунаправленным потоком данных между доменом авионики и другими доменами:
   - запрос, получение и агрегация данных из домена авионики;
   - отправка данных в домен авионики.
3. Сервер информационных приложений.
4. Безопасная фильтрация траффика из доменов связи, пилота, оператора и пассажиров.
5. Безопасные сетевые возможности для приложений и членов экипажа – каждый пользователь аутентифицируется с помощью логина/пароля, обладает определенными правами и в соответствии с ними имеет доступ только к тем приложениям, которые связанны с их правами.

Защищенный коммуникационный модуль выполняет следующие функции:

1. импорт, проверка целостности загрузки и хранение информации из домена с низким уровнем доверия (наземного) в домен со средним уровнем доверия (бортовые

Рис. 11. Связь киберпространства и физического мира

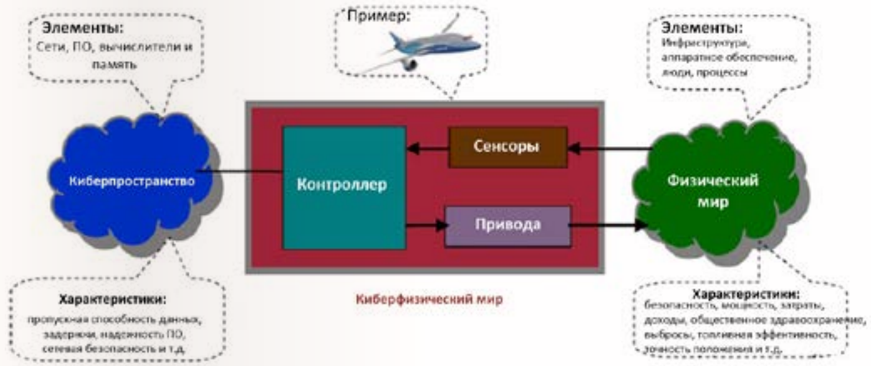


Рис. 12. Вопросы киберфизической безопасности

системы, кроме домена авионики);

2. безопасные сетевые возможности для приложений и членов экипажа – каждый пользователь аутентифицируется и обладает определенными правами, в соответствии с которыми имеет доступ только к выделенным приложениям;

3. безопасная фильтрация трафика и маршрутизация;

4. безопасное подключение к проводным интерфейсам.

Наличие серверов информации и приложений позволяет существенно расширить функциональность системы обеспечения ИБ за счет более низких требований к быстродействию и возможности глубокого анализа контекстной информации (рис. 10) [20].

Доступ к контексту информации обеспечивает возможность выхода за пределы чисто кибернетического пространства (рис. 11) и решения комплексных вопросов киберфизической безопасности на борту ВС, находящихся на стыке киберпространстве с физическим миром (рис. 12) [21].

Создание множественных независимых уровней безопасности (MLS – multilevel security) для обеспечения способности параллельно обрабатывать информацию разной степени защищенности в защищенном сервере реализуется с помощью гипервизора (рис. 13).

Программное ядро безопасности строится исходя из четырех фундаментальных политик:

- обеспечения допустимых информационных потоков между разделами;
- обеспечения изоляции данных разделов;
- обеспечения выполнения приложений в разделах в запланированные временны интервалы согласно временной диаграмме;
- обеспечения изоляция сбоев разделов.

В дополнение к этому предпринимаются специальные меры по минимизации неявных каналов коммуникации между приложениями (т.н. скрытые каналы). Современные реализации ядер безопасности на основе архитектуры MLS могут использовать аппаратные функции виртуализации, предоставляемые последними поколениями процессоров. Это позволяет, к примеру, реализовать гипервизор, способный выполнять гостевые ОС поверх ядра безопасности MLS в виртуализированной среде. Такой подход автоматически обеспечивает MLS-ядру изоляцию данных и контроль над информационными потоками, позволяя исключить появление скрытых каналов [22].

Заключение

Повышение уровня интеграции бортовой сети с внешними сетями и повсеместное внедрение беспроводных технологий передачи данных влечет за собой возрастающую потребность в предоставлении интегрированных сетевых вычислительных возможностей в сфере коммерческих перевозок для персонала, работающего на борту и обслуживающего воздушное судно, а также для пассажиров. Необходима такая вычислительная сеть, которая может быть соединена с наземными сетями, такими как Internet, локальные/глобальные (LANs/WANs) сети авиакомпаний и другие.

Рис. 13. Создание независимых уровней безопасности с помощью гипервизора

На сегодняшний день самым эффективным методом обеспечения информационной безопасности ВС является деление бортового оборудования на безопасные домены, с помощью которых можно четко установить границы, где обмен информацией должен отвечать наивысшим требованиям безопасности, в то время как другие домены могут иметь более низкий уровень доверия и взаимодействовать с сетями общего пользования, не беспокоясь о том, что потенциальные угрозы навредят критическим системам ВС.

В итоге можно наблюдать, что для обеспечения безопасной передачи данных необходимо и достаточно разместить на борту интеллектуальные устройства безопасности во всех местах, где происходит стыковка систем.

Обеспечение ИБ с помощью отдельных бортовых защищенных устройств характеризуется следующими основными преимуществами: отсутствие повышения нагрузки на центральные бортовые вычислители из-за программно-аппаратной поддержки функций обеспечения ИБ; возможность реализации механизмов обеспечения программной и аппаратной отказоустойчивости при возникновении угроз ИБ.

В результате бортовые системы смогут быстро и безопасно соединяться с внешними сетями, увеличить эффективность обмена данными благодаря более широкой полосе пропускания (например, совместное использование частот для беспроводных систем), а также облегчить доступность к бортовым системам для обслуживающего и технического персонала.

Литература

1. Sampigethaya K. et al. Future e-enabled aircraft communications and security: The next 20 years and beyond // Proceedings of the IEEE. 2011. Т. 99. №. 11. С. 2040-2055.

2. Wolf M., Minzlaff M., Moser M. Information technology security threats to modern e-enabled aircraft: A cautionary note // Journal of Aerospace Information Systems. 2014. Т. 11. №. 7. С. 447–457.

3. Зыбин Е.Ю., Косьянчук В.В., Сельвесюк Н.И. Электрификация и интеллектуализация – основные тенденции развития энергокомплекса воздушных судов // Авиационные системы. 2016. №5. С. 45–51.

4. Зыбин Е.Ю., Косьянчук В.В. Эволюция архитектуры комплекса бортового оборудования воздушных судов // IV Юбилейная Всероссийская научно-техническая конференция «Авиационные системы в XXI веке», посвященная 70-летию со дня создания ФГУП «ГосНИИАС», сб. тезисов, 26–27 мая 2016 г., г. Москва. 2016. С. 198.

5. Федосов Е.А., Чуянов Г.А., Косьянчук В.В., Сельвесюк Н.И. Перспективный облик и технологии разработки комплексов бортового оборудования воздушных судов // Полет. 2013. № 8. С. 41–52.

6. Желтов С.Ю., Косьянчук В.В., Сельвесюк Н.И. Перспективы интеллектуализации современных авиационных комплексов // В сборнике: Материалы пленарного заседания 7-й Российской мультиконференции по проблемам управления ОАО «Концерн «ЦНИИ «Электроприбор». 2014. С. 54–60.

7. Чуянов Г.А., Косьянчук В.В., Сельвесюк Н.И., Кравченко С.В. Направления совершенствования бортового оборудования для повышения безопасности полетов воздушного судна // Известия ЮФУ. Технические науки. 2014. № 6 (155). С. 219–229.

8. Chuyanov G.A., Kosyanchuk V.V., Selvesyuk N.I., Zybin E.Yu. Advanced avionics equipment on the basis of second generation integrated modular avionics // 29th Congress of the International Council of the Aeronautical Sciences, ICAS 2014. ICAS 2014 CD-ROM Proceedings. 2014.

9. Зыбин Е.Ю., Косьянчук В.В., Сельвесюк Н.И. Отказоустойчивая архитектура комплексных систем управления перспективных самолетов транспортной категории на базе единой вычислительной платформы // Тезисы докладов Третьей Всероссийской научно-технической конференции «Навигация, наведение и управление летательными аппаратами». М.: Издательство «Научтехлитиздат», 2017. С. 227–229.

10. Sampigethaya K., Poovendran R., Bushnell L. Secure operation, control, and maintenance of future e-enabled airplanes // Proceedings of the IEEE. 2008. Т. 96. №. 12. С. 1992-2007.

11. Olive M. L., Oishi R. T., Arentz S. Commercial aircraft information security-an overview of arinc report 811 // 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA. IEEE, 2006. С. 1-12.

12. Reiger M. P. R., Strigini L., Bloomfield R. Evidence-Based Security in Aerospace.

13. Batuwangala E. et al. Safety and security considerations in the certification of next generation avionics and air traffic management systems // 17th Australian International Aerospace Congress: AIAC 2017. Engineers Australia, Royal Aeronautical Society, 2017. С. 440.

14. Strohmeier M. et al. On perception and reality in wireless air traffic communication security // IEEE transactions on intelligent transportation systems. 2017. Т. 18. №. 6. – С. 1338-1357.

15. Mahmoud M. S. B., Pirovano A., Larrieu N. Aeronautical communication transition from analog to digital data: A network security survey // Computer Science Review. 2014. Т. 11. С. 1-29.

16. Галушкин В.В., Катков Д.И., Косьянчук В.В., Сельвесюк Н.И. Технология создания комплексов бортового оборудования воздушных судов // В книге: Навигация, наведение и управление летательными аппаратами. Всероссийская научно-техническая конференция. К 65-летию ОАО «Раменское приборостроительное конструкторское бюро». 2012. С. 171–174.

17. Сельвесюк Н.И., Косьянчук В.В. Основные подходы при разработке авионики для авиации общего назначения // В книге: Навигация, наведение и управление летательными аппаратами. Материалы Второй Всероссийской научно-технической конференции. 2015. С. 251–253.

18. Галушкин В.В., Катков Д.И., Косьянчук В.В., Сельвесюк Н.И. Сквозная технология проектирования комплексов бортового оборудования перспективных воздушных судов // Известия ЮФУ. Технические науки. 2012. № 3 (128). С. 201–209.

19. Tubis A., Werbińska-Wojciechowska S. The scope of the collected data for a holistic risk assessment performance in the road freight transport companies // Advances in Dependability Engineering of Complex Systems. Springer, Cham, 2017. С. 450-463.

20. Lu T. et al. A Security Architecture in Cyber- Physical Systems: Security Theories, Analysis, Simulation and Application Fields // International Journal of Security and Its Applications. – 2015. Т. 9. №. 7. С. 1–16.

21. Sampigethaya K., Poovendran R. Aviation cyber–physical systems: Foundations for future aircraft and air transport // Proceedings of the IEEE. 2013. Т. 101. №. 8. С. 1834-1855.

22. Baker A., River W. High Assurance Systems Development Using the MILS Architecture.