КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БОРТОВОГО ОБОРУДОВАНИЯ ВОЗДУШНОГО СУДНА

Косьянчук В.В.[1], Сельвесюк Н.И.[2], Зыбин Е.Ю.[3], Хамматов Р.Р.[4], Карпенко С.С.[5]

Цель работы: *анализ текущего уровня и разработка новых подходов к обеспечению информационной безопасности воздушных судов.*

Метод исследования: *методы компаративного и теоретико-сравнительного анализа на основе принципов системности. Проводится анализ тенденций информатизации и интеграции бортового оборудования, показана информационная архитектура и инфраструктура современного воздушного судна, рассмотрены инциденты и потенциальные уязвимости информационной безопасности в авиации.*

Результаты: *разработана концепция обеспечения информационной безопасности бортового оборудования воздушного судна как на этапе его разработки, так и на этапе эксплуатации. На этапе разработки информационная безопасность должна обеспечиваться за счет применения сквозных технологий проектирования, в том числе с использованием автоматизированных средств. Обеспечение информационной безопасности при эксплуатации обеспечивается за счет разделения информационно-вычислительной сети воздушного судна по уровням доверия на безопасные контролируемые домены с разной степенью защищенности и внедрения между ними дополнительных средств защиты: бортового защищенного шлюза и бортовых защищенных серверов. Бортовой защищенный шлюз представляет собой межсетевой экран, осуществляющий контроль сетевого траффика, поступающего в наиболее защищенный домен авионики. Бортовые защищенные серверы управляют двунаправленными потоками данных между авионикой и внешней средой и обеспечивают хранение всей потенциально недостоверной информации, доступ к которой может получить каждый из доменов. В состав бортового защищенного сервера входят: защищенный коммуникационный модуль, сервер информации и серверы приложений. Наличие серверов информации и приложений позволяет существенно расширить функциональность системы обеспечения информационной безопасности за счет возможности глубокого анализа контекста информации. Это позволяет выйти за пределы чисто кибернетического пространства и решать комплексные задачи обеспечения киберфизической безопасности на борту воздушного судна, находящиеся на стыке киберпространства с физическим миром[6].*

Ключевые слова: *кибербезопасность на воздушном транспорте, интеллектуализация бортового оборудования, несанкционированный доступ, уязвимости информационной безопасности, информационно-вычислительное пространство, информационные домены, архитектура комплекса бортового оборудования.*

DOI: 10.21681/2311-3456-2018-4-9-20

Введение

Для повышения эффективности гражданских перевозок на перспективных воздушных судах (ВС) должны использоваться технологии и процессы для увеличения пропускной способности каналов передачи данных. Такие ВС с поддержкой постоянной связи (E-enabled) будут играть ключевую роль в будущем [1]. Кроме обеспечения эффективной интеграции воздушных и наземных сетей необходимо обеспечить высокий уровень информационной безопасности ВС. В данной работе предлагается новая концепция построения бортовой информационно-вычислительной сети ВС, позволяющая разделить информационно-вычислительное пространство ВС по уровням доверия с целью безопасного обмена данными на борту ВС и за его пределами.

Развитие информационно-вычислительных сетей ВС

Традиционно воздушное судно (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 микроэлектрони-

1 Косьянчук Владислав Викторович, доктор технических наук, профессор РАН, ФГУП «ГосНИИАС», Первый заместитель генерального директора, Москва, Россия, E-mail: vvk@gosniias.ru

2 Сельвесюк Николай Иванович, доктор технических наук, профессор РАН, ФГУП «ГосНИИАС», заместитель генерального директора, Москва, Россия, E-mail: nis@gosniias.ru

3 Зыбин Евгений Юрьевич, доктор технических наук, ФГУП «ГосНИИАС», начальник лаборатории, Москва, Россия, E-mail: eyzybin@2100.gosniias.ru

4 Хамматов Рашит Рифович, кандидат технических наук, ФГУП «ГосНИИАС», ведущий инженер, Москва, Россия, E-mail: rrhammatov@2100.gosniias.ru

5 Карпенко Сергей Сергеевич, ФГУП «ГосНИИАС», инженер, Москва, Россия, E-mail: kss@gosniias.ru

6 Исследование выполнено при финансовой поддержке РФФИ (гранты 17-08-01445а, 18-08-00453а)

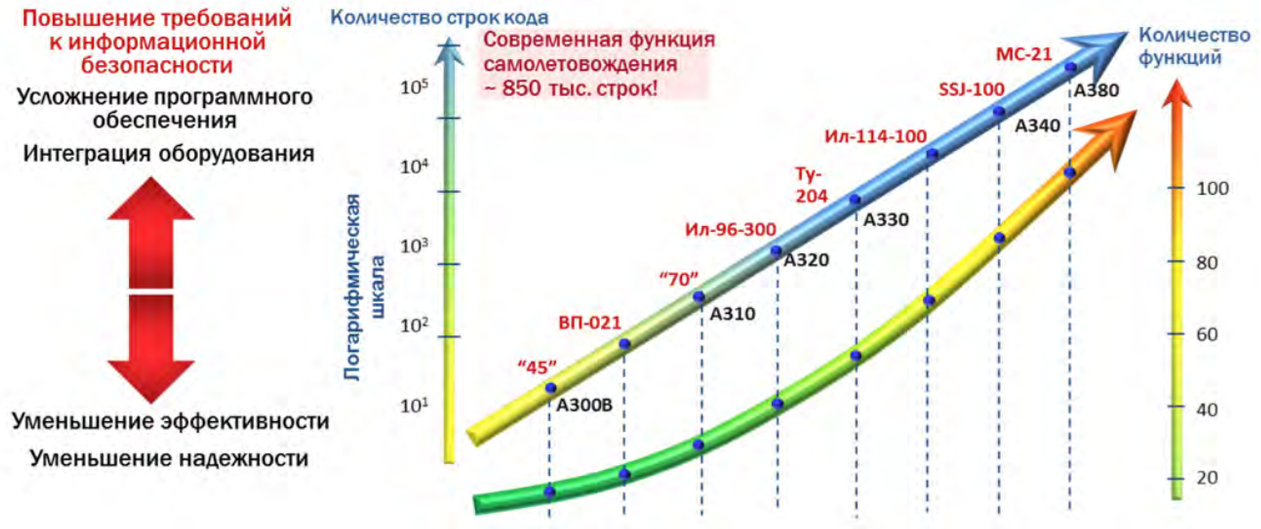

Рис. 1. Тенденции информатизации воздушных судов

ки, 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 борту ВС (рис. 1) [1–6].

Развитие микроэлектроники и вычислительной техники, их интенсивное проникновение в авиационную электронику обуславливали постоянное развитие и создание качественно новых поколений КБО (рис. 2) [2–4, 7].

Распределённый 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 электро-

Рис. 2. Развитие архитектуры бортового оборудования воздушных судов

тельная система ВС разделяется на информационные домены с разной степенью защищенности [1]:

- домен управления ВС (закрытый);
- домен информационных услуг воздушного судна (достоверный);
- домен бортовой развлекательно-информационной системы (общественный).

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 (ИМА) [8–10]. 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

ники, питания графики и видео, обусловили повышение степени внутренней информационной связности ВС [4–9]. 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-вычисли-

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

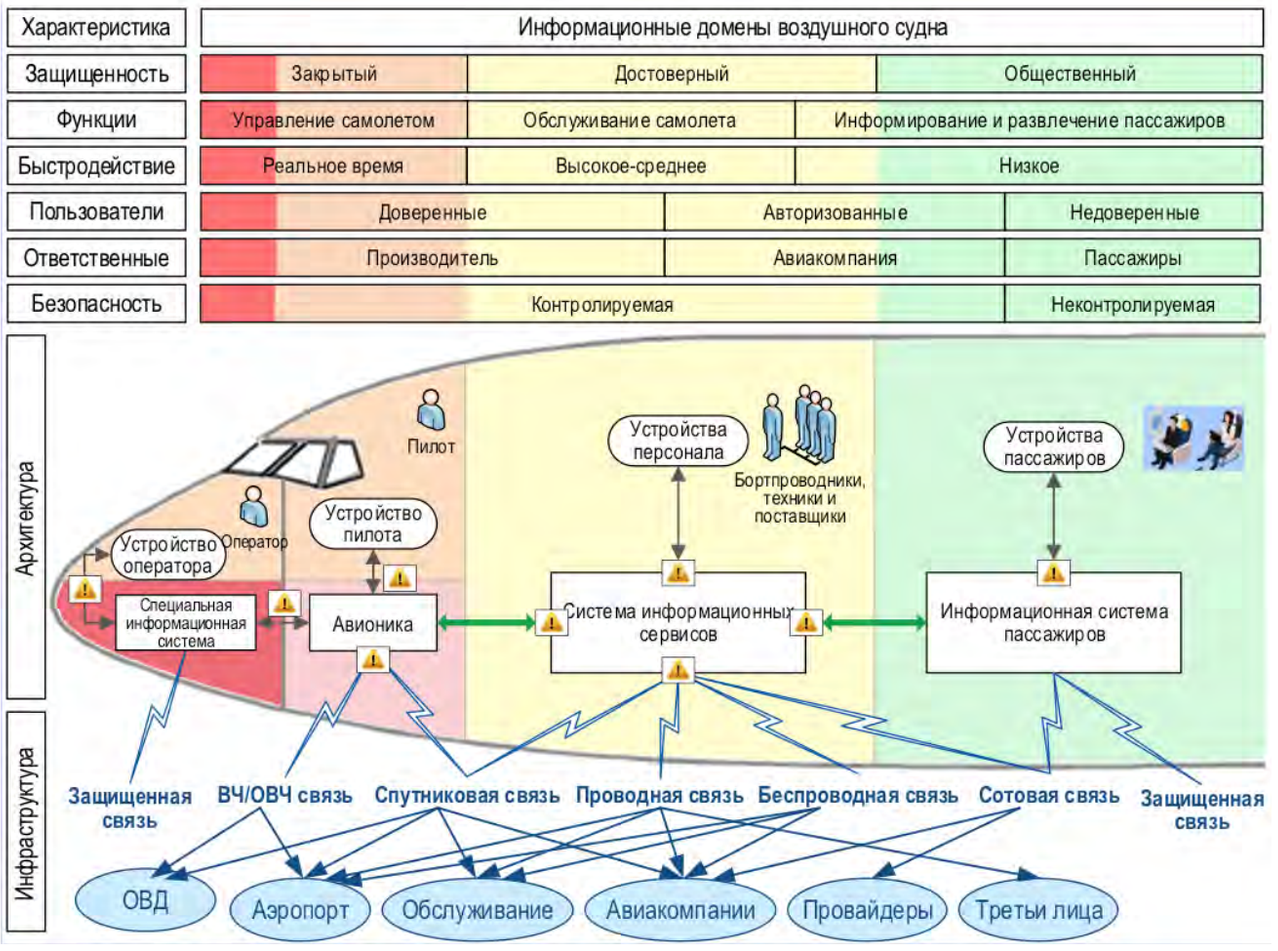

Рис. 3. Информационная архитектура и инфраструктура ВС

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

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 самолётовождения, данных коммерческого характера и т.п., которые негативно сказываются 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 авиации (табл.1, 2) [11– 13].

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.

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, выполняющие критически важные операции, необходимые для обеспечения безопасности полета	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

– 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.).

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

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

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

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 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 [14–16].

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) :

– 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 траффика и обеспечивающий защищенную связь между доменом авионики и внешней средой.

Бортовой защищенный шлюз выполняет следующие функции: трансляцию протоколов домена авионики и информационного домена; инспекцию состояния информационной безопасности; безопасную управляемую коммутацию. Для трансляции протоколов в шлюзе используются заголовки всех транслируемых протоколов.

Инспекция состояния информационной безопасности осуществляется за счет (рис. 6): безопасной маршрутизации; фильтрации траффика из не доверенных доменов; использованием посредников прикладного уровня; регистрации событий информационной безопасности.

В защищенном шлюзе реализованы различные наборы прокси-серверов и служб аутентификации, которые по-

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 5000	более 5000

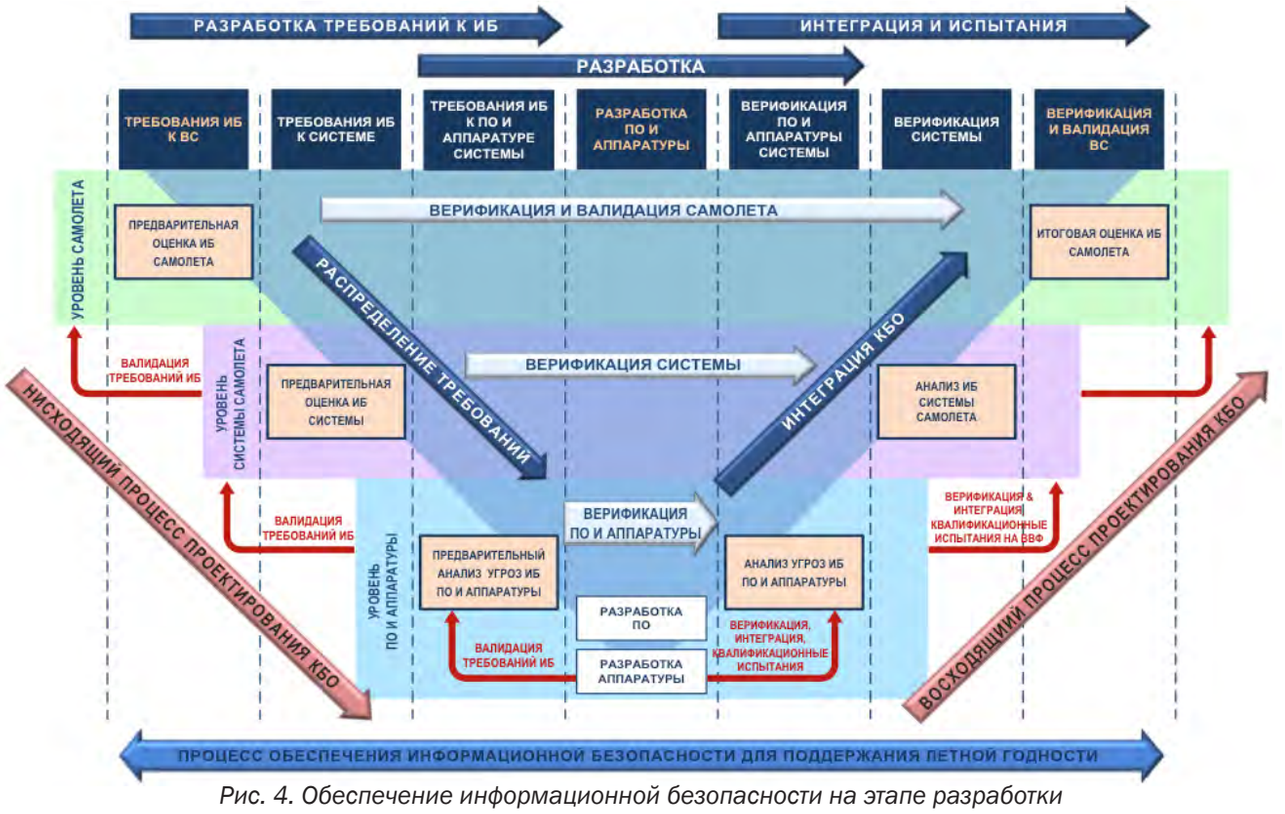

Рис. 4. Обеспечение информационной безопасности на этапе разработки

зволяют 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.

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 [17].

В состав бортового защищенного сервера входят (рис. 7):

– защищенный коммуникационный модуль;

– сервер информации;

– серверы приложений.

Защищенный коммуникационный модуль выполняет следующие функции:

– импорт, проверка целостности загрузки и хранение информации из домена с низким уровнем доверия (наземного) в домен со средним уровнем доверия (бортовые системы, кроме домена авионики);

– 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;

– безопасная фильтрация траффика и маршрутизация;

– 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. 8) [18].

Доступ к контексту информации обеспечивает возможность выхода за пределы чисто кибернетического пространства и решения комплексных вопросов киберфизической безопасности на борту ВС, находящихся на стыке киберпространстве с физическим миром (рис. 9) [18, 19].

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

Программное ядро безопасности строится исходя из четырёх фундаментальных политик:

– обеспечения допустимых информационных потоков между разделами;

– обеспечения изоляции данных разделов;

– обеспечения выполнения приложений в разделах

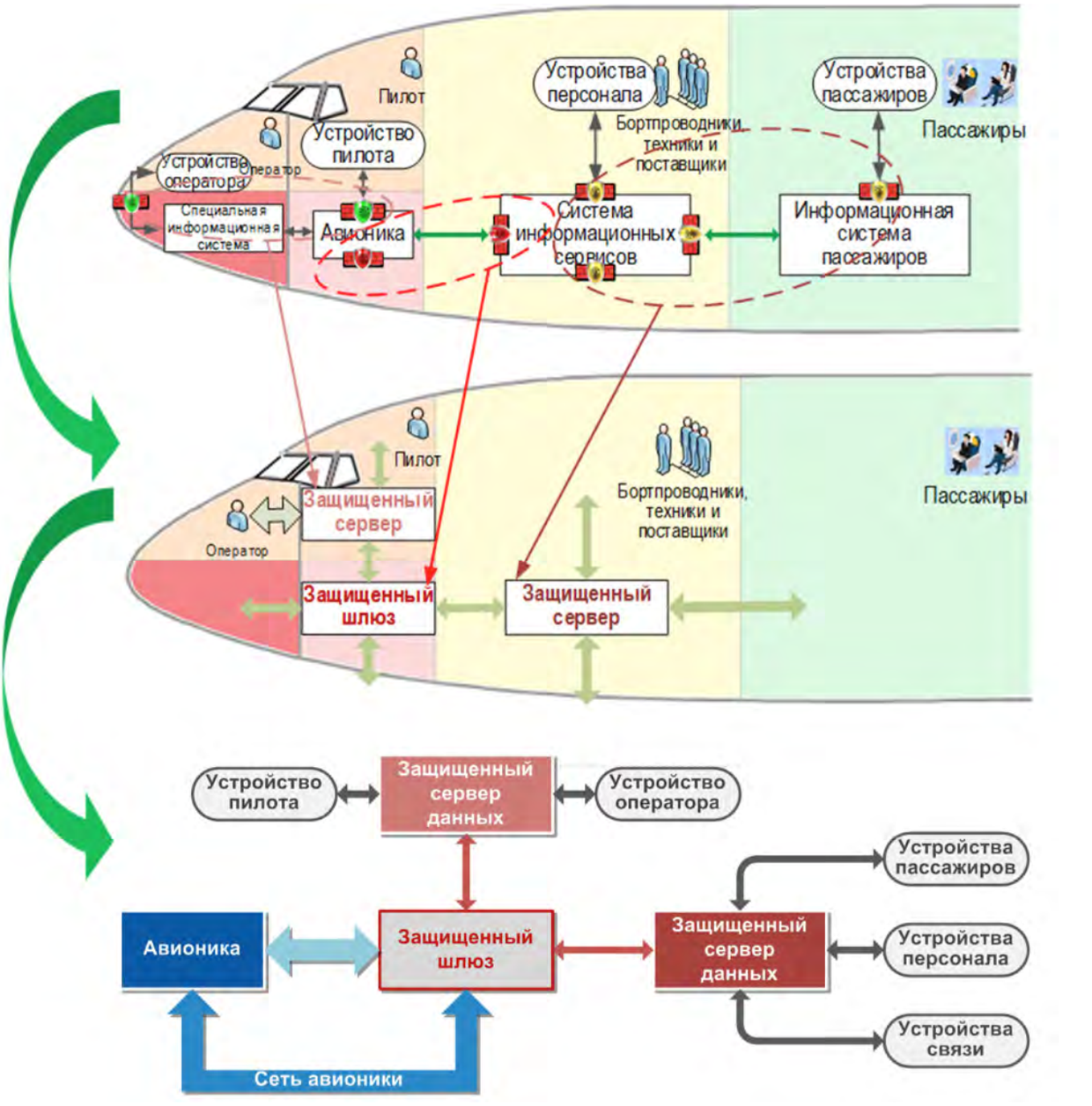

Рис. 5. Архитектура информационной безопасности воздушного судна.

Рис. 6. Принцип работы бортового защищенного шлюза

Рис. 7. Состав и принцип работы бортового защищенного сервера

в запланированные временные 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 информационны-

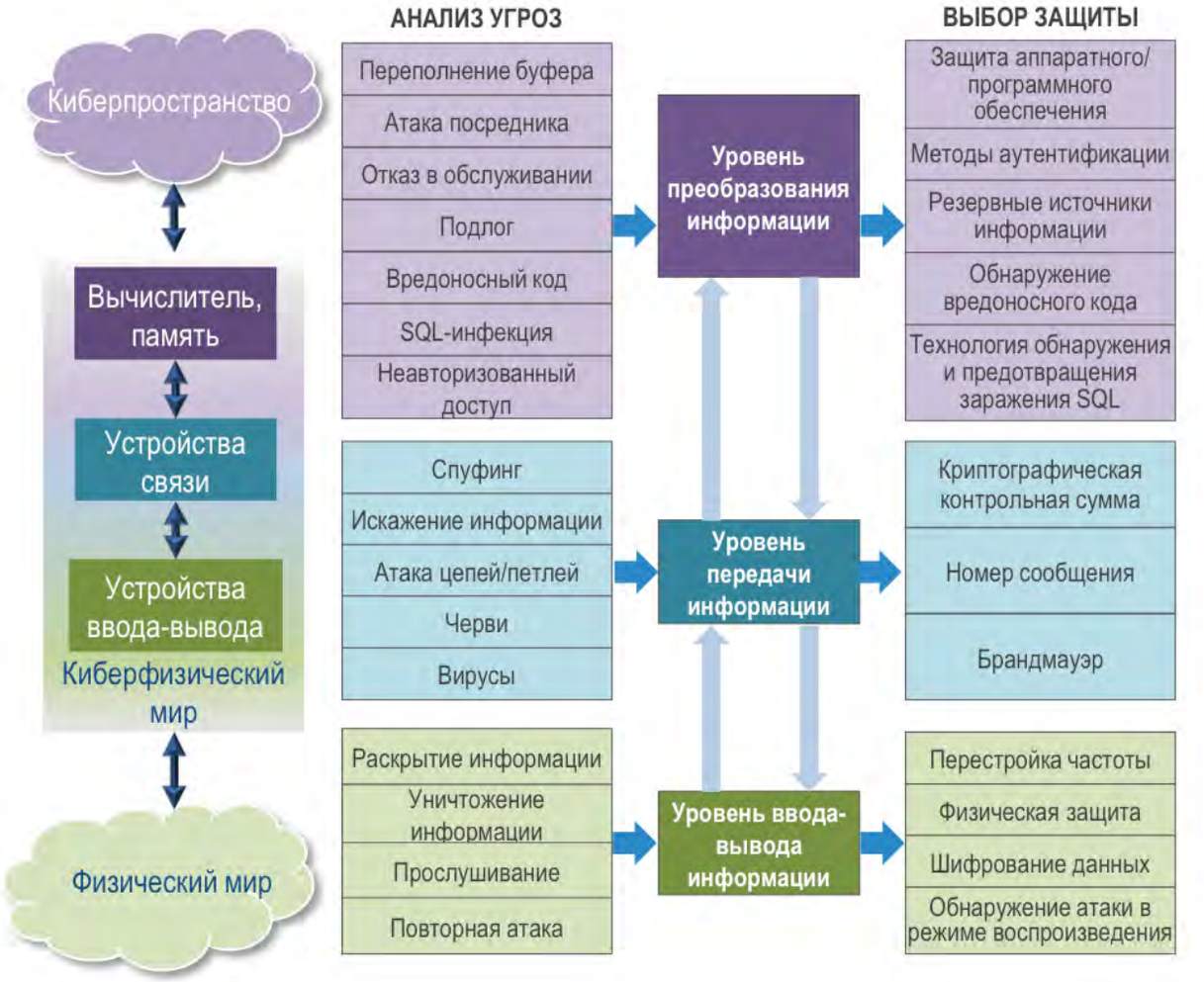

Рис. 8. Принцип работы бортового защищенного сервера

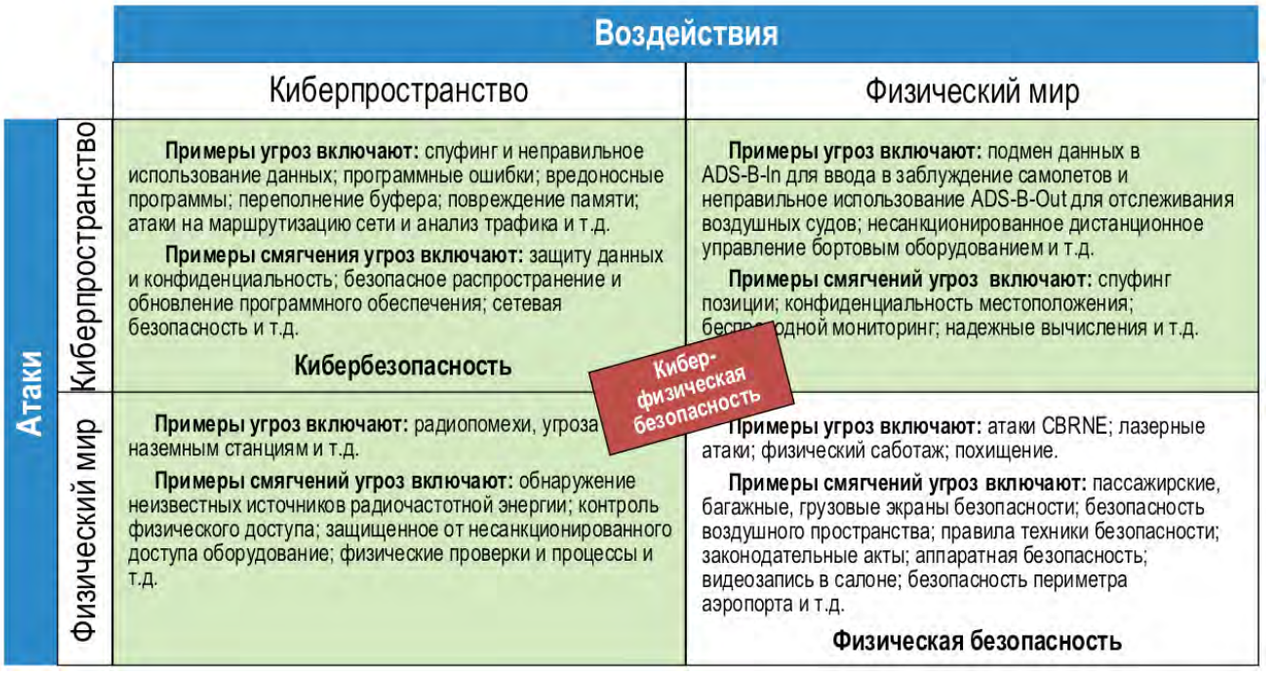

Рис. 9. Вопросы киберфизической безопасности

ми потоками, позволяя исключить появление скрытых каналов [20].

Заключение

Внедрение предлагаемых методов обеспечения информационной безопасности на борту ВС позволит сохранить надежность авиационных систем на высоком уровне, предотвратить несчастные случаи на воздушном транспорте и улучшить качество предоставляемых услуг.

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 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.

Рецензент: *Соколов Владимир Николаевич, доктор технических наук, профессор, заместитель Главного конструктора ФГУ МОКБ "Марс", г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. 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.
2. 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.
3. 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», сборник докладов, 26–27 мая 2016 г., г. Москва. 2017. С. 19–28.
4. 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.
5. Желтов С.Ю., Косьянчук В.В. Перспективы интеллектуализации современных авиационных комплексов // Вестник Российской академии наук. 2018. Т. 88. № 2. С. 107–117.

6. Желтов С.Ю., Косьянчук В.В., Сельвесюк Н.И. Перспективы интеллектуализации современных авиационных комплексов // Авиационные системы. 2016. № 5. С. 38-45.
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. Косьянчук В.В., Зыбин Е.Ю., Карпенко С.С., Бондаренко Ю.В. Резервированная интегрированная система мониторинга технического состояния воздушного судна // В книге: Девятый международный аэрокосмический конгресс IAC18 Тезисы докладов. 2018. С. 119–121.
11. 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. P. 440.
12. Strohmeier M. et al. On perception and reality in wireless air traffic communication security // IEEE transactions on intelligent transportation systems. 2017. Vol. 18. No. 6. P. 1338–1357.
13. Mahmoud M. S. B., Pirovano A., Larrieu N. Aeronautical communication transition from analog to digital data: A network security survey // Computer Science Review. 2014. Vol. 11. P. 1–29.
14. Федосов Е.А., Косьянчук В.В., Сельвесюк Н. Интегрированная модульная авионика // Радиоэлектронные технологии. 2015. № 1. С. 66–71.
15. 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.
16. Косьянчук В.В., Сельвесюк Н.И. Новая функциональность бортового оборудования воздушных судов // Материалы 10-й Всероссийской мультиконференции по проблемам управления МКПУ-2017. 2017. С. 139–141.
17. 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. P. 450–463.
18. 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. Vol. 9. No. 7. P. 1–16.
19. Sampigethaya K., Poovendran R. Aviation cyber–physical systems: Foundations for future aircraft and air transport // Proceedings of the IEEE. 2013. Vol. 101. No. 8. P. 1834–1855.
20. Jungwirth P., Chan P., Barnett T., Badawy A. H. Cyber defense through hardware security // Disruptive Technologies in Information Sciences. International Society for Optics and Photonics, 2018. Vol. 10652. P. 106520P.

THE CONCEPT FOR INFORMATION SECURITY OF AIRCRAFT EQUIPMENT

Kosyanchuk V.[1], Selvesyuk N.[2], Zybin E.[3], Khammatov R.[4], Karpenko S.[5]

Purpose: Analysis of the current level of and developing new approaches to aircraft information security.

Research methods: Comparative and theoretical/comparative analysis methods based on the principles of consistency. Aircraft equipment computerization and integration trends are analyzed, modern aircraft's information architecture and infrastructure are shown, incidents and potential IS vulnerabilities in aviation are discussed.

Results: A concept was developed for aircraft equipment information security both at the design and operation stages. At the design stage, information security should rely on end-to-end design technologies, including those using automated tools. In operation, information security is provided by dividing the aircraft computer network by trust levels

1 Vladislav Viktorovich Kosyanchuk, Doctor of Technical Sciences, Professor of the Russian Academy of Sciences, FSUE "GosNIIAS", First Deputy Director General, Moscow, Russia. E-mail: vvk@gosniias.ru

2 Nikolay Ivanovich Selvesyuk, Doctor of Technical Sciences, Professor of the Russian Academy of Sciences, FSUE "GosNIIAS", Deputy Director General, Moscow, Russia. E-mail: nis@gosniias.ru

3 Eugene Yurievich Zybin, Doctor of Technical Sciences, FSUE "GosNIIAS", Head of Laboratory, Moscow, Russia. E-mail: eyzybin@2100.gosniias.ru

4 Rashit Rifovich Khammatov, Ph.D., FSUE "GosNIIAS", Leading Engineer, Moscow, Russia. E-mail: rrhammatov@2100.gosniias.ru

5 Sergey Sergeevich Karpenko, FSUE "GosNIIAS", Engineer, Moscow, Russia. E-mail: kss@gosniias.ru

into controlled secure domains with varying degrees of security and by disposing additional protections (onboard secure gateway and onboard secure servers) among them. The onboard secure gateway is a firewall that monitors the network traffic entering the most secure domain of the avionics. The onboard secure servers control bi-directional data flows between the avionics and the external environment and store all potentially unreliable information that can be accessed by each of the domains. An onboard secure server comprises a secure communication module, information server and application servers. The information servers and applications help significantly expand the information security system's functionality through in-depth analysis of the information context. This makes it possible to go beyond purely cyberspace and deal with complex tasks of onboard cyber-physical security at the interface of cyberspace with the physical world.

Keywords: cyber security, air transport, avionics intellectualization, avionics architecture, unauthorized access, information security vulnerabilities, information and computing space, information domains.[6]

References

1. Wolf M., Minzlaff M., Moser M. Information technology security threats to modern e-enabled aircraft: A cautionary note // Journal of Aerospace Information Systems. 2014. Vol. 11. No. 7. P. 447–457.
2. Zybin E.Yu., Kosyanchuk V.V., Selvesyuk N.I. Elektrifikaciya i intellektualizaciya – osnovnye tendencii razvitiya energokompleksa vozdushnyh sudov // Aviacionnye sistemy. 2016. No. 5. P. 45–51.
3. Zybin E.Yu., Kosyanchuk V.V. Evolyuciya arhitektury kompleksa bortovogo oborudovaniya vozdushnyh sudov // IV Yubilejnaya Vserossijskaya nauchno-tekhnicheskaya konferenciya «Aviacionnye sistemy v XXI veke», posvyashchennaya 70-letiyu so dnya sozdaniya FGUP «GosNIIAS», sb. tezisov, 26–27 maya 2016 g., g. Moskva. 2016. P. 198.
4. Fedosov E.A., Chuyanov G.A., Kosyanchuk V.V., Selvesyuk N.I. Perspektivnyj oblik i tekhnologii razrabotki kompleksov bortovogo oborudovaniya vozdushnyh sudov // Polet. 2013. No. 8. P. 41–52.
5. Zheltov S.Yu., Kosyanchuk V.V. Perspektivy intellektualizacii sovremennyh aviacionnyh kompleksov // Herald of the Russian Academy of Sciences. 2018. Vol. 88. No. 2. P. 107–117.
6. Zheltov S.Yu., Kosyanchuk V.V., Selvesyuk N.I. Perspektivy intellektualizacii sovremennyh aviacionnyh kompleksov // Aviatsionnyye sistemy. 2016. No. 5. P. 38–45.
7. Chuyanov G.A., Kosyanchuk V.V., Selvesyuk N.I., Kravchenko S.V. Napravleniya sovershenstvovaniya bortovogo oborudovaniya dlya povysheniya bezopasnosti poletov vozdushnogo sudna // Izvestiya YUFU. Tekhnicheskie nauki. 2014. No. 6 (155). P. 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. Zybin E.Yu., Kosyanchuk V.V., Selvesyuk N.I. Otkazoustojchivaya arhitektura kompleksnyh sistem upravleniya perspektivnyh samoletov transportnoj kategorii na baze edinoj vychislitel'noj platformy // Tezisy dokladov Tret'ej Vserossijskoj nauchno-tekhnicheskoj konferencii «Navigaciya, navedenie i upravlenie letatel'nymi apparatami». M.: Izdatel'stvo «Nauchtekhlitizdat», 2017. P. 227–229.
10. Kosyanchuk V.V., Zybin E.Yu., Karpenko S.S., Bondarenko Yu.V. Rezervirovannaya integrirovannaya sistema monitoringa tekhnicheskogo sostoyaniya vozdushnogo sudna // Devyatyy mezhdunarodnyy aerokosmicheskiy kongress IAC18 Tezisy dokladov. 2018. P. 119–121.
11. 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. P. 440.
12. Strohmeier M. et al. On perception and reality in wireless air traffic communication security // IEEE transactions on intelligent transportation systems. 2017. Vol. 18. No. 6. P. 1338–1357.
13. Mahmoud M. S. B., Pirovano A., Larrieu N. Aeronautical communication transition from analog to digital data: A network security survey // Computer Science Review. 2014. Vol. 11. No. 1–29.
14. Fedosov E.A., Kosyanchuk V.V., Selvesyuk N.I. Integrirovannaya modul'naya avionika // Radioelektronnyye tekhnologii. 2015. No. 1. P. 66–71.
15. Sel'vesyuk N.I., Kos'yanchuk V.V. Osnovnye podhody pri razrabotke avioniki dlya aviacii obshchego naznacheniya // V knige: Navigaciya, navedenie i upravlenie letatel'nymi apparatami. Materialy Vtoroj Vserossijskoj nauchno-tekhnicheskoj konferencii. 2015. P. 251–253.
16. Kosyanchuk V.V., Selvesyuk N.I. Novaya funktsional'nost' bortovogo oborudovaniya vozdushnykh sudov // Materialy desyatoy Vserossiyskoy mul'tikonferentsii po problemam upravleniya MKPU-2017. 2017. P. 139–141.
17. 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. P. 450–463.
18. 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. Vol. 9. No. 7. P. 1–16.
19. Sampigethaya K., Poovendran R. Aviation cyber–physical systems: Foundations for future aircraft and air transport // Proceedings of the IEEE. 2013. Vol. 101. No. 8. P. 1834–1855.
20. Jungwirth P., Chan P., Barnett T., Badawy A. H. Cyber defense through hardware security // Disruptive Technologies in Information Sciences. International Society for Optics and Photonics, 2018. Vol. 10652. P. 106520P.

6 The study was supported by the Russian Foundation for Basic Research (grants 17-08-01445a, 18-08-00453a)