Приведем некоторые примеры, для которых может подойти данное программно-аппаратное средство:

1. Экзаминация обучающихся для передачи отдельных пакетов данных с материалами для прохождения аттестации с расшифрованием данных в назначенное время.

2. Обновление лицензии программного обеспечения без необходимости пересылки идентификатора лицензии в открытом виде или трудоемкой повторной доставке данной информации.

Данные варианты подразумевают пересылку по открытому каналу передачи данных определенного количества файлов соответствующего количеству ключей, хранящихся на токене, для последующего последовательного их расшифрования.

Вывод. За счет предварительного распространения ключевых параметров *m, k* обеих сторон обеспечивается аутентификация ключей, случайный выбор *x* и *y* гарантирует, что обе стороны могут быть уверены в создании нового сессионного ключа в каждом сеансе протокола [6].

Реализация протокола с применением криптографических токенов является наглядной и понятной схемой для конечного пользователя.

Литература

1. Diffie, W. New Directions in Cryptography / W. Diffie, M. Hellman // IEEE Transactions on Information Theory. – 1976. – Vol. 22, № 6. – P. 644–654.

2. Лебедев, А. Н. Способ рассылки защищенных данных с регулированием доступа к отдельным их разделам / А. Н. Лебедев // Вопросы кибербезопасности. – 2015. – Т. 13, № 5. – С. 70–72.

3. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. NIST. – [Электронный ресурс]. Режим доступа: https://nvlpubs.nist.gov. – Дата доступа: 21.04.2021.

4. Лебедев, А. Н. Обобщенный протокол Диффи-Хеллмана с аутентификацией сторон / А. Н. Лебедев // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. – М. : МГУ, 2018. – С. 123–127.

5. Лебедев, А. Н. Новые арифметические операции конечного коммутативного кольца и их использование в криптографии / А. Н. Лебедев // Безопасные информационные технологии : сборник трудов IX Всероссийской научно-технической конференции. – Москва, 2018. – 8 с.

6. Matsumoto, T. On seeking smart publickey-distribution systems / T. Matsumoto, Y. Takashima, H. Imai // Trans. Inst. Electron. Commun. Eng. Jpn. Sect. E. – 1986. – Vol. 69,№ 2. – P. 99–106.

УДК 004.056

ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЛЕКСА БОРТОВОГО ОБОРУДОВАНИЯ ГРАЖДАНСКОГО ВОЗДУШНОГО СУДНА НА БАЗЕ ОТКРЫТОЙ СЕТЕВОЙ АРХИТЕКТУРЫ

Медведев Н.В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Предлагаются принципы построения защищенного комплекса управления гражданского воздушного судна, основанные на трех информационных доменах и открытой сетевой структуре.
Ключевые слова: гражданское воздушное судно, информационный домен, защищенный сервер, единая информационно-вычислительная платформа, комплекс.

CONSTRUCTION PRINCIPLES OF A CIVIL AIRCRAFT COMPLEX BASED ON OPEN NETWORK ARCHITECTURE

Medvedev N.

Bauman State Technical University
Moscow, Russia

Abstract. The principles of building a secure civil aircraft control complex based on three information domains and an open network structure are proposed.
Key words: civil aircraft, information domain, secure server, unified information and computing platform, complex.
Адрес для переписки: Медведев Н.В., ул. Вторая Бауманская, 5, г. Москва 105005, Российская Федерация
e-mail: medvedevnick54@yandex.ru

Современные распределенный и интегрированный принципы построения комплекса бортового оборудования гражданского воздушного судна (БО ГВС) на базе открытой сетевой архитектуры и единой информационно-вычислительной платформы обусловили повышение степени внутренней информационной связности ГВС [1]. Это существенно повысило степень внешней информационной связности ГВС и привело к появлению концепции информационного связанного (E-enabled) ВС с поддержкой внешних сервисов, как показано на рис. 1 [2].

Связанным воздушным судам необходимо быть самостоятельными узлами в Авиационных самоорганизующихся сетях (AANET), повсеместно общаясь с наземной инфраструктурой и други-

ми бортами. Увеличение информационных потоков от самолетов к земле, от земли к самолетам, между самолетами при помощи AANET позволит повысить безопасность полетов, точность расписания, эффективность обслуживания, уровень обслуживания пассажиров, как показано на рис. 2.

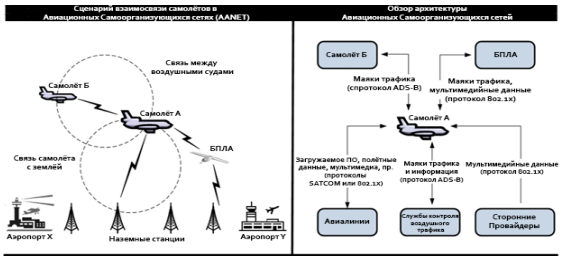

Рисунок 1 – Связанные воздушные суда

Рисунок 2 – Открытая сетевая архитектура

В соответствии с международными стандартами ARINC 811, ARINC 664 единая информационно-вычислительная платформа ВС разделяется на информационные домены с разной степенью защищенности [1] (рис. 3):

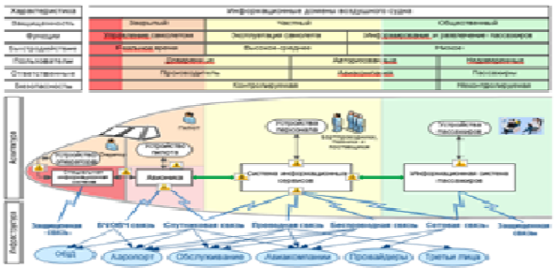

Рисунок 3 – Доменная структура управления ГВС

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

Домен бортовой развлекательно-информационной системы предоставляет развлекательные услуги и информацию о полете пассажирам. Включает в себя два домена: домен информационной системы пассажиров и домен пассажирских устройств. Для разделения информационно-вычислительной платформы по уровням доверия на безопасные контролируемые домены между ними внедряются дополнительные аппаратные средства защиты: бортовой защищенный шлюз и бортовые защищенные сервера.

Одно из главных требований в гражданской авиации – обеспечение международной интероперабельности с учетом реальной оснащенности воздушных судов, наземной инфраструктуры. А это серьезно ограничивает использование технологий обеспечения информационной безопасности. Для защиты предполагается применение криптографических средств, включая открытое распределение ключей. Некриптографические методы, как показывает анализ сложившейся ситуации, зачастую оставляют заметные уязвимости в системе безопасности.

Важнейшим моментом является гармонизация подходов под эгидой ИКАО. В 2019 году на кибер-саммите ИКАО получила подтверждение необходимости криптозащиты цифровых и голосовых сообщений в системе управления воздушным движением. Исходя из взаимодействия беспилотных воздушных судов (БВС) с пилотом дистанционно-пилотируемых авиационных систем (ДПАС) и системой УВД и с учетом требований по кибербезопасности, эти факторы предопределяют структуру и технические характеристики средств интеграции ДПАС в общее воздушное пространство.

Использование беспроводных технологий подразумевает доступ к радиосвязи. Например, на борту планируется использовать мобильные телефоны, лэптопы, RFID-тэги, повышающие угрозу несанкционированного доступа к беспроводным узлам «связанного» самолета.

Общей целью «врага» может считаться получение привилегированного доступа к операциям «связанного» самолета путем атаки информационных активов. Враг для сети может быть внешним и внутренним. Он может использовать пассивные атаки (анализ сетевого трафика) и активные атаки (создавать ложный узел, компрометировать информацию от сенсоров). Предполагается, что злоумышленник может глушить беспроводные каналы.

Для того чтобы в процессе разработки комплекса БО ГВС была заложена защита от угроз кибербезопасности, необходимо руководствоваться помимо указанных международных стандартов также стандартами в области защиты информации. Главным стандартом в данной области является стандарт ГОСТ Р ИСО/МЭК 15408, состоящий из трех частей и регламентирующий стадии и содержание разработки требований к проектированию ПО. Комплекс БО ГВС представляет собой

интеллектуальную защищенную автоматизированную систему, обеспечивающее хранение всей информации из внешней среды, доступ к которой может получить каждый из доменов.

Комплекс призван выполнять следующие функции:

– сервер информационных приложений;

– управление двунаправленным потоком данных между доменом авионики и другими доменами;

– безопасная фильтрация трафика из доменов связи, пилота, оператора и пассажиров;

– безопасные сетевые возможности для приложений и членов экипажа.

В состав комплекса входят: защищенный коммуникационный модуль; сервер информации; серверы приложений.

Сервер информации и серверы приложений обеспечивают хранение всей информации из внешней среды, доступ к которой может получить каждый из доменов, а также реализацию внешних сервисов, предоставляемыми диспетчерскими службами, авиакомпаниями, производителями и третьими лицами.

Защищенный коммуникационный модуль включает в свой состав универсальный интеграционный шлюз и универсальный шлюз безопасности. Шлюз безопасности предназначен для решения большинства вопросов кибербезопасности, связанных с поддержкой информационно-вычислительной платформы внешних сервисов.

Литература

1. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна / В.В. Косьянчук [и др.] // Вопросы кибербезопасности. – 2018. – Т. 28, № 4. – С. 9–20.

2. Документы ИКАО – Библиотека – Авиационный портал [Электронный ресурс]. – Режим доступа: https://airspot.ru/library/dokumenty-ikao – Дата доступа: 01.10.2021.

3. Управление инспекции по безопасности полетов РФ/Анализ состояния безопасности полетов в граждан-ской авиации в 2018 году [Электронный ресурс]. – Режим доступа: https://dvmtu-favt.ru. – Дата доступа: 20.08.2021.

4. Воздушный кодекс РФ от 19.03.1997 N 60-ФЗ [Электронный ресурс]. – Режим доступа: https://consultant.ru. – Дата доступа: 25.07.2021.

УДК 53.082

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ДЕГРАДАЦИИ ЛАКОКРАСОЧНЫХ ПОКРЫТИЙ ЗОНДОВЫМ ЗАРЯДОЧУВСТВИТЕЛЬНЫМ МЕТОДОМ

Микитевич В.А., Пантелеев К.В., Жарин А.Л.

Белорусский национальный технический университет
Минск, Республика Беларусь

Аннотация. Исследованы процессы деградации лакокрасочного покрытия на металлической подложке при воздействии раствора соли. Анализ поверхности выполнен зондовым зарядочувствительным методом. Получены карты распределения потенциала поверхности. Выявлена корреляция между потенциалом поверхности и типом дефекта лакокрасочного покрытия.

Ключевые слова: потенциал поверхности, лакокрасочное покрытие, деградация покрытия.

STUDY OF THE PROCESSES OF DEGRADATION OF PAINT COATINGS BY THE PROBE CHARGING SENSITIVE METHOD

Mikitsevich U., Pantsialeyeu K., Zharin A.

Belarusian National Technical University
Minsk, Belarus

Abstract. The processes of degradation of a paint coating on a metal substrate after exposure to a salt solution have been investigated. The analysis of the surface was carried out using a charge-sensitive probe method. The maps of the surface potential distribution are obtained. A correlation was found between the surface potential and the type of paintwork defect.

Key words: surface potential, paint coating, coating degradation.

Адрес для переписки: Микитевич В.А., пр. Независимости, 65, г. Минск 220113, Республика Беларусь
e-mail: mikitevichva@bntu.by

Введение. Широкое применение лакокрасочных покрытий требует проведение исследования качества покрытий. Стандартные методы испытания основаны на исследовании длительного воздействия неблагоприятных факторов с последующей визуальной оценкой по бальной шкале.

В настоящее время зондовые зарядочувствительные методы измерения находят все более широкое применение. Зондовые методы применяются не только для исследования поверхностей металлов и полупроводников [1], но для исследования полимеров [2, 3]. Особенность