УДК 629.7.017.01:771.64

ПОСТРОЕНИЕ СИСТЕМЫ КРИПТОЗАЩИЩЁННОГО ОБМЕНА ИНФОРМАЦИЕЙ О ЛЁТНОЙ ГОДНОСТИ ВС

А.К. БЛАГОРАЗУМОВ, Ю.И. ЕВДОКИМОВ, И.Г. КИРПИЧЕВ

Описаны проблемы и решения построения системы информационного обмена, предоставляющей субъектам ГА возможность безопасной передачи через Интернет данных о технической эксплуатации ВС.

Ключевые слова: лётная годность, ИАС МЛГ ВС, передача данных, криптографическая защита информации, ЭЦП, удостоверяющий центр.

Введение

Одним из условий обеспечения конкурентоспособности отечественных воздушных судов (ВС) является совершенствование системы поддержания их лётной годности и послепродажного обслуживания. С 2001 г. в ГосНИИ ГА ведётся разработка Информационно-аналитической системы мониторинга летной годности воздушных судов (ИАС МЛГ ВС) [1], которая призвана объединить эксплуатантов, конструкторов, изготовителей ВС, поставщиков изделий авиационной техники, организации по ТОиР и авиационные власти в единое информационное пространство технической эксплуатации ВС.

Неотъемлемой составляющей единого информационного пространства является налаженная система передачи информации о лётном и техническом состоянии ВС. По мере распространения Интернета появилась возможность его использования для более оперативной и надёжной передачи данных по сравнению с их пересылкой на физических носителях. Но, как было показано в [2], передача данных через Интернет между защищёнными сетевыми экранами организациями вызывает определённые сложности, пропорциональные объёму передаваемых файлов.

Для решения проблем обмена данными с сервером ИАС МЛГ ВС в Информационно-аналитическом центре (ИАЦ) ГосНИИ ГА был разработан метод передачи данных через крипто-туннель [3], который за полтора года был внедрён в 18-ти организациях и на практике доказал свою надёжность и эффективность.

Часть пользователей ИАС МЛГ ВС работает также с другими информационными системами и программным обеспечением (ПО), требующими распределённой обработки информации, доступ к которой жёстко регламентируется. В качестве примера можно привести обработку данных бортовых средств объективного контроля. В процессе внедрения ИАС МЛГ ВС эти пользователи проявили заинтересованность в системе информационного обмена, позволяющей доставлять данные конкретным исполнителям с защитой от перехвата и фальсификации.

Для удовлетворения потребностей таких пользователей в ИАЦ ГосНИИ ГА было принято решение расширить функциональность существующей системы информационного обмена, предоставив пользователям возможность передавать не только данные ИАС МЛГ ВС, но и обмениваться произвольными данными между собой. Проектирование новой системы потребовало анализа и учёта требований проявивших заинтересованность организаций.

Анализ требований к системе информационного обмена

По статистике сервера ИАС МЛГ ВС типичный размер файла данных о состоянии ВС находится в диапазоне 2-30 Мбайт, в семи процентах случаев превышая 500 Мбайт. В трети случаев передача файла занимает более часа. Часть пользователей подключается к Интернету через

сотовые модемы, испытывая обрывы связи в процессе передачи файлов. Как следствие, ПО обмена должно обладать устойчивостью к обрывам связи, автоматически восстанавливая соединение и возобновляя передачу данных.

Эффективность системы напрямую зависит от возможностей автоматизации обмена данными и интеграции с существующими информационными системами. Для её повышения ПО обмена должно предоставлять программный интерфейс управления передачей файлов.

В настоящее время оптимизированные для передачи больших файлов сетевые протоколы, как правило, блокируются корпоративными сетевыми экранами. Требование их разблокирования может вступить в противоречие с корпоративной политикой сетевой безопасности. Таким образом, ПО обмена должно уметь выполнять свои транспортные функции, используя только разрешённые сетевые протоколы.

Поскольку вышеприведённым требованиям удовлетворяет уже отработанный в ИАЦ ГосНИИ ГА метод передачи данных через крипто-туннель [3], он был выбран в качестве транспортного протокола проектируемой системы. Этот метод использует авторизацию с помощью ключей RSA или DSA и шифрует передаваемые данные по одному из алгоритмов AES, Blowfish или 3DES [4]. Однако факт шифрования посредством разработанного в США ПО был негативно воспринят, в частности, руководством гражданской авиации Республики Куба, являющейся одним из основных импортеров российских самолётов. По их мнению, криптостойкость этого ПО могла быть умышленно понижена для предоставления спецслужбам США возможности дешифрования перехваченных данных за приемлемое время. Как следствие, к системе было предъявлено требование шифрования информации по сертифицированным российским криптоалгоритмам.

Масштабируемость системы и её открытость для подключения новых участников выдвигает требование надёжной и однозначной идентификации отправителя конкретного файла, исключающей любую возможность отправки данных от чужого имени.

Для исключения потерь или искажения данных (включая их умышленную подмену) по пути от отправителя до получателя требуется наличие контроля целостности данных.

Далее рассматриваются возможные способы защиты данных и структура информационного обмена, удовлетворяющие предъявленным требованиям.

Защита передаваемых данных от перехвата

Решение задачи защиты передаваемой информации от перехвата третьими лицами было найдено в использовании шифрования по алгоритмам, специфицированным в ГОСТ 28147-89 [5] посредством российского ПО, сертифицированного Федеральной службой безопасности России. Конкретный пакет ПО шифрования выбирался по критериям распространённости и длительности присутствия на рынке, что косвенно свидетельствует о надёжности ПО и его совместимости с широким спектром операционных систем и программных окружений. Предпочтение было отдано ПО КриптоПро CSP, имеющему выданный ФСБ России сертификат соответствия СФ/114-1453 от 01.04.2010г. Это ПО разработано основанной в 2000г. компанией "Крипто-Про" (www.cryptopro.ru), имеющей лицензию ФСБ России на разработку криптографических средств № 8711П от 22.04.2010г. КриптоПро CSP производит шифрование и дешифрование по алгоритму ГОСТ 28147-89 через программный интерфейс Microsoft Windows. Однако, выполняя функцию криптопровайдера, КриптоПро CSP не имеет графического пользовательского интерфейса для непосредственной работы с файлами. Этот пробел заполняет пакет "КриптоАРМ", имеющий сертификат соответствия ФСБ России № СФ/114-1712 от 20.09.2011г., созданный российской компанией "Цифровые Технологии" (www.trusted.ru), имеющей лицензию ФСБ России на разработку криптографических средств № 5394П от 17.04.2008г.

Схема передачи файлов с использованием функции шифрования КриптоАрм посредством криптопровайдера КриптоПро CSP изображена на рис. 1.

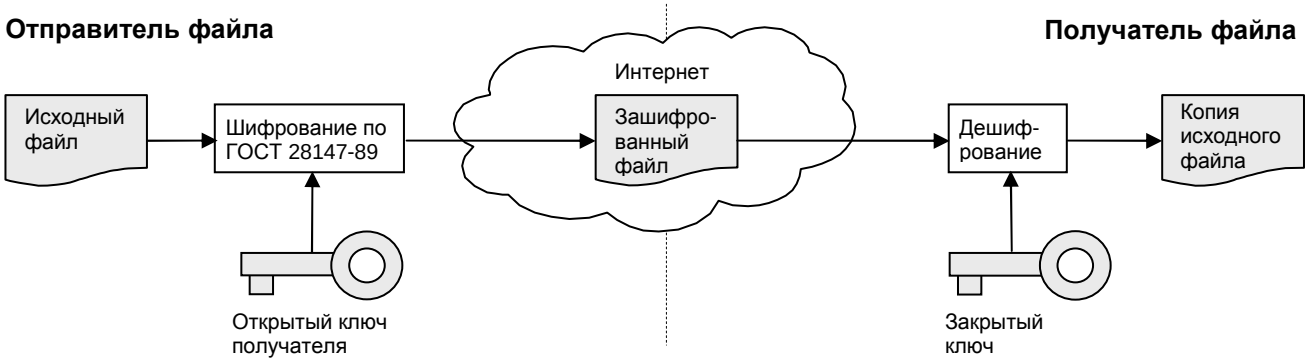

Рис. 1. Передача файлов с шифрованием

Такое шифрование, широко известное как "криптография с открытым ключом", основывается на выбранной паре ключей шифрования. Для шифрования используется открытый (публичный) ключ получателя, свободно предоставляемый всем потенциальным отправителям. Дешифрование же возможно только посредством закрытого (секретного) ключа получателя, хранимого последним в тайне от всех. По открытому ключу невозможно вычислить необходимый для дешифрования закрытый ключ.

На практике КриптоАрм не шифрует файл непосредственно открытым ключом. Вместо этого сначала генерируется вспомогательный случайный ключ, используемый для блочного шифрование файла по ГОСТ 28147-89. Вспомогательный ключ является симметричным, т.е. им же можно дешифровать файл. После шифрования файла вспомогательным ключом последний шифруется открытым ключом получателя и добавляется к передаваемому файлу. Не меняя сути шифрования с открытым ключом, такой алгоритм имеет следующие преимущества:

- блочное симметричное шифрование осуществляется во много раз быстрей асимметричного;
- отправляя файл нескольким получателям не надо шифровать его персонально для каждого достаточно добавить несколько байт персонально зашифрованного вспомогательного ключа.

У каждого участника обмена должны присутствовать открытые ключи всех потенциальных получателей. Эти ключи могут быть легко извлечены из компьютера стандартными средствами операционной системы. Как следствие, это алгоритм, обеспечивая надёжную защиту информации от перехвата, не способен достоверно идентифицировать отправителя, допуская создание успешно дешифруемого файла посторонним лицом. Другими словами, одного только шифрования по ГОСТ 28147-89 не достаточно для защиты передаваемых данных от фальсификации.

Защита передаваемых данных от искажения и подмены

Задача контроля целостности данных и подтверждения их авторства была решена использованием электронной цифровой подписи (ЭЦП), имеющей юридическую силу на основании Федерального закона от 10 января 2002 г. № 1-ФЗ и пришедшего ему на смену Федерального закона от 6 апреля 2011 г. № 63-ФЗ. Схема передачи файла, дополненная процедурами формирования и проверки ЭЦП, приведена на рис. 2.

Прикрепление и проверка ЭЦП осуществляется по алгоритму ГОСТ Р 34.10-2001 [6], суть которого в следующем:

- для файла по алгоритму ГОСТ Р 34.11-94 [7] вычисляется хэш-функция (своеобразный "отпечаток пальца"), которая шифруется закрытым ключом отправителя и добавляется к файлу;
- получатель отделяет ЭЦП от файла, самостоятельно вычисляет хэш-функцию файла и сравнивает её с хэш-функцией, дешифрованной открытым ключом отправителя из ЭЦП.

Совпадение хэш-функцией свидетельствует о том, что ЭЦП была создана именно тем отправителем, чей открытый ключ использовался для проверки ЭЦП.

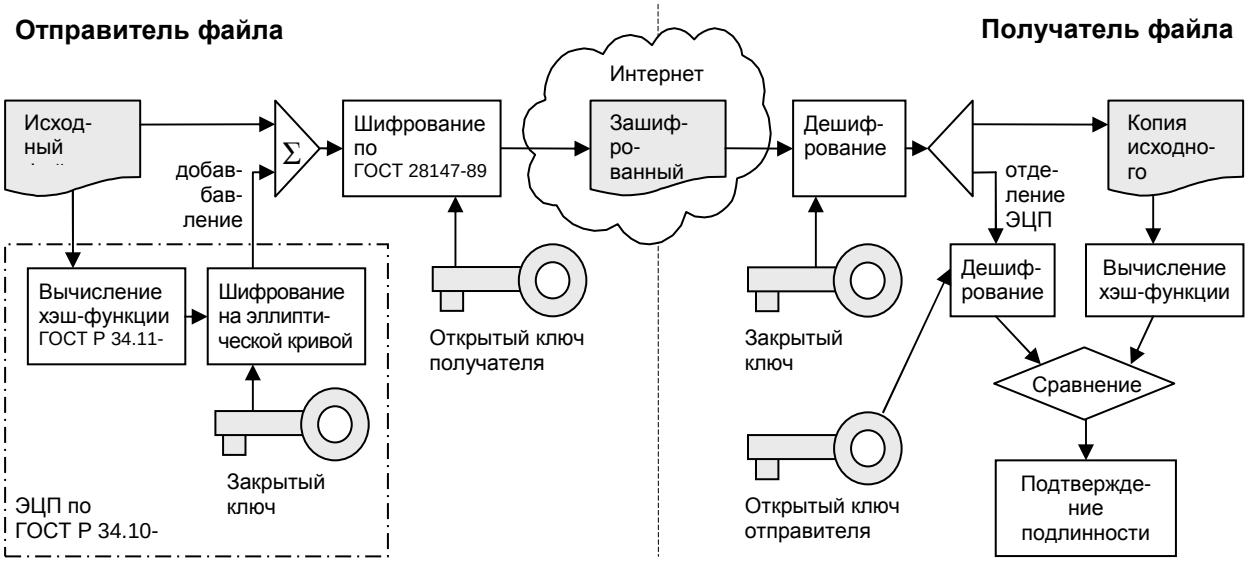

Рис. 2. Передача файлов с шифрованием и проверкой подлинности отправителя

Для того чтобы официально ассоциировать открытый ключ с конкретным юридическим или физическим лицом, используются сертификаты открытых ключей, специфицированные в рекомендации X.509 Международного союза по телекоммуникациям (International Telecommunication Union, ITU) и документе RFC 3280 Организации инженерной поддержки Интернета (Internet Engineering Task Force, IETF). Сертификат издаётся удостоверяющим центром, который генерирует для каждого пользователя пару взаимосвязанных ключей. Закрытый ключ передаётся только будущему владельцу, как правило, записанным на токене, представляющем собой похожее на USB-флешку устройство, чтение из которого выполняется специализированными программами. Открытый ключ вместе с идентифицирующей владельца информацией записывается в файл сертификата и подписывается ЭЦП удостоверяющего центра.

Сертификаты участников информационного обмена могут выдаваться удостоверяющим центром ГосНИИ ГА, имеющем лицензию на предоставление услуг в области шифрования информации № 9131 от 15.07.2010, выданную Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

Структура и функционирование системы информационного обмена

Построить систему, в которой каждый участник обмена может передавать данные напрямую другому участнику, можно, только если их компьютеры всегда готовы принимать сетевые подключения со стороны Интернета. Но обычно компьютеры корпоративных пользователей закрыты от внешних подключений сетевыми экранами, включены только треть суток, располагаясь при этом в разных часовых поясах.

В этих условиях единственным решением является использование клиент-серверной архитектуры с постоянно доступным для всех сервером, принимающим файлы у отправителей и предоставляющим возможность их скачивания получателями (рис. 3). Такой сервер был установлен в дата-центре ИАЦ ГосНИИ ГА. Наличие сервера-посредника не сказывается на безопасности обмена, т.к. передаваемые данные могут быть дешифрованы исключительно конечными получателями, а ЭЦП надёжно защищает их от подмены.

Сервер обмена обслуживает соединения по двум сетевым протоколам:

– SSH (англ. Secure SHell - безопасная оболочка);

– HTTP (англ. HyperText Transfer Protocol - протокол передачи гипертекста).

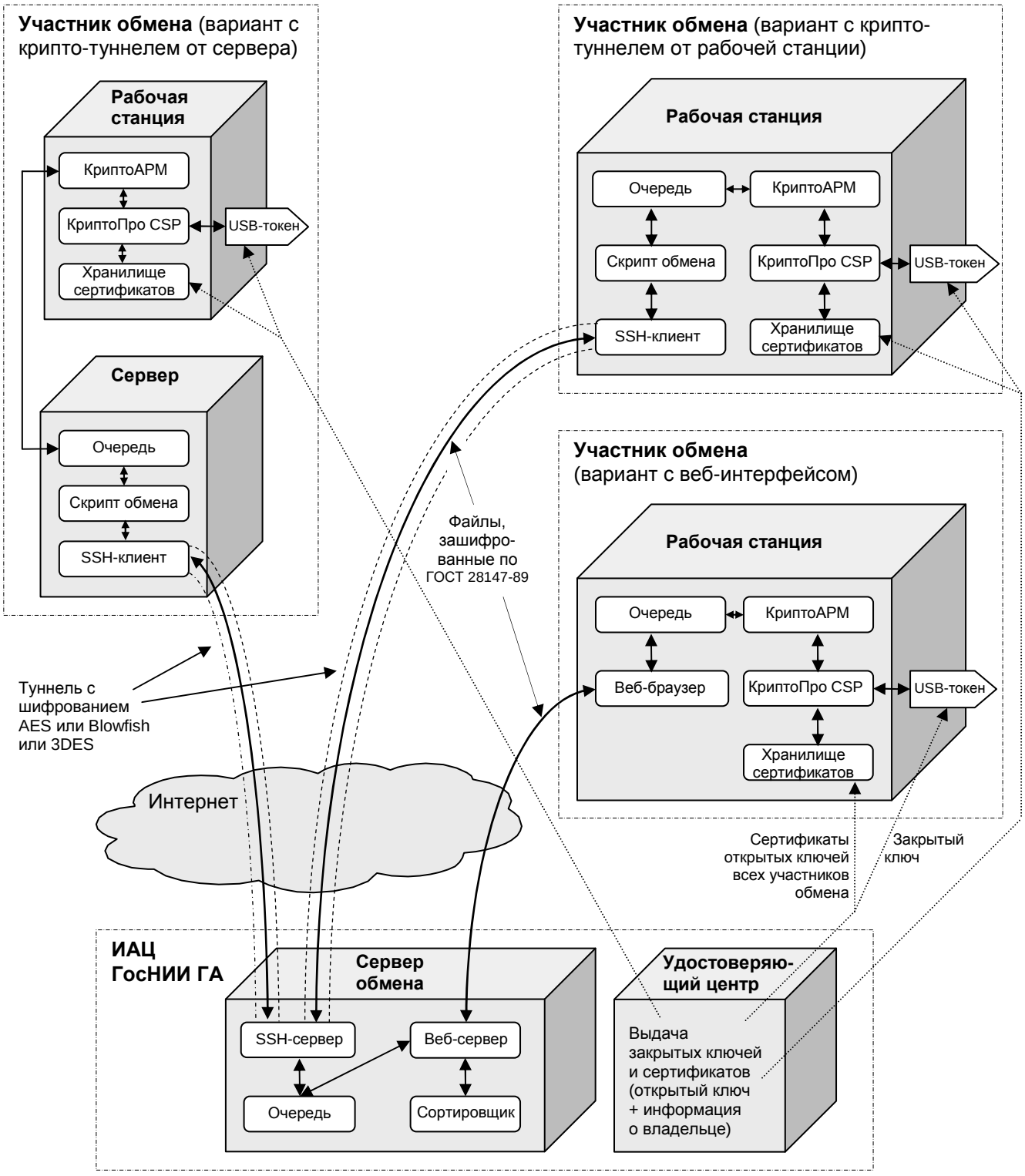

Рис. 3. Схема информационного взаимодействия

Отправка файла начинается с прикрепления ЭЦП отправителя и шифрования посредством КриптоАРМ с сохранением результирующего файла в папку очереди на отправку. Для создания ЭЦП к компьютеру должен быть подключен USB-токен с закрытым ключом отправителя. Имя сохраняемого файла должно содержать код получателя, используемый для сортировки файлов на сервере обмена.

Установлением соединений с сервером обмена и передачей файлов управляет описанный в [3] скрипт – пошагово интерпретируемая программа. Скрипт обмена может запускаться как с

сервера (рис. 3, вверху слева), так и с рабочей станции (рис. 3, вверху справа). Первый вариант оптимален, когда в организации есть несколько пользователей, передающих данные, объём которых соизмерим с пропускной способностью Интернет-канала. Этот вариант позволяет задействовать Интернет-канал и в нерабочее время, при выключенных рабочих станциях.

Скрипт обмена извлекает файлы из очереди на отправку и разбивает их на пакеты, передача которых повторяется в случае обрыва связи. Посредством SSH-клиента скрипт соединяется с SSH-сервером, принимающим подключения на TCP-порту 443, обычно задействованном протоколом HTTPS (англ. HTTP Secure – "безопасный протокол передачи гипертекста"). Использование этого порта позволяет избежать блокирования трафика сетевыми экранами [2].

В каждом сеансе соединения с сервером скрипт обмена проверяет наличие адресованных пользователю пакетов и загружает их на его компьютер (или на сетевой диск – в варианте, когда скрипт обмена работает на сервере). В дальнейшем пакеты собираются в файл, дешифруемый с помощью КриптоАРМ с подключенным USB-токеном.

При наличии хорошего Интернет-канала и нерегулярном обмене небольшими объёмами данных пользователи могут работать с веб-интерфейсом сервера обмена, получая к нему доступ по HTTP-протоколу из обычного Интернет-браузера (рис. 3, справа посередине). В этом случае процедуры шифрования и дешифрования файлов аналогичны вышеописанным.

Сервер обмена содержит папки входящих и исходящих файлов для каждого пользователя, доступные для работающих служб SSH-сервера и веб-сервера (рис. 3, внизу). Периодически запускаемый скрипт сортировщика перекладывает загруженные файлы в папки получателей по их коду, указанному в имени файла. Попутно скрипт преобразует файлы (передаваемые по HTTP) в пакеты (передаваемые по SSH) и наоборот.

Процедура подключения к системе информационного обмена нового пользователя заключается в установке на его компьютер ПО КриптоПро CSP и КриптоАРМ, а также получении от удостоверяющего центра ГосНИИ ГА USB-токена с закрытым ключом и сертификатов открытого ключа всех участников обмена. При этом удостоверяющий центр рассылает сертификат нового пользователя всем остальным участникам обмена.

Заключение

Описанная система информационного обмена была разработана в строгом соответствии с российскими ГОСТами. Реализация элементов криптографии на сертифицированном ФСБ России ПО гарантирует защиту передаваемых данных от перехвата и фальсификации. Система легко масштабируется: добавление новых корреспондентов не требует ни изменения сетевых настроек, ни приобретения дополнительных лицензий на средства криптографической защиты.

Система прошла апробацию, показав хорошие результаты, при налаживании обмена с кубинской авиакомпанией "Cubana de Aviación S.A." информацией о техническом и лётном состоянии эксплуатируемых на Кубе самолётов Ил-96 и Ту-204. Эта авиакомпания испытывала множество технических и организационных проблем со связью, обусловленных очень строгими требования к информационной безопасности и медленным (средняя скорость – 56Кбит/с) подключением к Интернету через цепочку фильтрующих трафик серверов вышестоящих организаций ГА и органов государственной безопасности.

В процессе трехмесячного тестирования были выявлены и устранены отдельные недостатки реализации описанного в [3] алгоритма, в частности ложное принятие решения об отсутствии файлов в очереди при невозможности получения их списка в момент обрыва связи.

Как результат, в настоящее время ИАЦ ГосНИИ ГА имеет отлаженную технологическую платформу, позволяющую подключать все заинтересованные субъекты ГА к обмену информацией о техническом и ресурсном состоянии ВС.

ЛИТЕРАТУРА

1. Кирпичев И.Г., Кулешов А.А., Шапкин В.С. Основы построения и функциональности развития информационно-аналитической системы мониторинга жизненного цикла компонентов воздушных судов. - М.: ГосНИИ ГА, 2008.

2. Благоразумов А.К., Кирпичев И.Г. Способы передачи данных в ИАС МЛГ ВС через Интернет // Научный Вестник МГТУ ГА. - 2011. - № 163.

3. Благоразумов А.К., Кирпичев И.Г. Автоматизация информационного обмена в ИАС МЛГ ВС // Научный Вестник МГТУ ГА. - 2011. - № 163.

4. Константин Стародубцев. Вмешательство на расстоянии // Chip Special. - М.: Издательский дом "Бурда", 2004. - № 8. - С. 76-81.

5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. - Введ. 1989-06-02. - М.: Издательство стандартов, 1996.

6. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. - Взамен ГОСТ Р 34.10-94. - Введ. 2002-07-01. - М.: Госстандарт России, 2001.

7. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. - Введ. 1994-05-23. - М.: Госстандарт России, 1994.

IMPLEMENTATION OF A SYSTEM OF ENCRYPTED EXCHANGE OF AIRWORTHINESS DATA

Blagorazumov A.K., Evdokimov Y.I., Kirpichev I.G.

This article describes problems and solutions of implementation of a data exchange system, which enables civil aviation organizations to securely transfer aircraft airworthiness data through the Internet.

Key words: airworthiness, information system, data exchange, cryptography, digital signature, certification authority.

Сведения об авторах

Благоразумов Андрей Кириллович, 1970 г.р., окончил МАИ (1992), начальник группы Информационно-аналитического центра ГосНИИ ГА, автор 6 научных работ, область научных интересов – информационные технологии.

Евдокимов Юрий Иванович, 1961 г.р., окончил МИИГА (1984), начальник Управления поддержания летной годности гражданских воздушных судов Федерального агентства воздушного транспорта, автор 3 научных работ, область научных интересов – поддержание лётной годности и сертификация воздушных судов.

Кирпичев Игорь Геннадьевич, 1960 г.р., окончил МИИГА (1986), доктор технических наук, заместитель генерального директора - директор Информационно-аналитического центра ГосНИИ ГА, эксперт Межгосударственного авиационного комитета, автор более 40 научных работ, область научных интересов – информационные системы, сопровождение технической эксплуатации авиационной техники.