УДК ???

ЗАЩИТА ДАННЫХ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ МОНИТОРИНГА ЛЕТНОЙ ГОДНОСТИ ВОЗДУШНЫХ СУДОВ

И.Г. КИРПИЧЕВ, А.К. БЛАГОРАЗУМОВ

Описаны методы, используемые в Информационно-аналитической системе мониторинга лётной годности воздушных судов (ИАС МЛГ ВС) для защиты данных в процессе их передачи через интернет между субъектами ИАС МЛГ ВС, а также при хранении и обработке на серверах центральной базы данных ИАС МЛГ ВС.

Ключевые слова: ИАС МЛГ ВС, передача данных, шифрование, отказоустойчивость, виртуализация

Введение

В основу построения ИАС МЛГ ВС положен принцип создания единого информационного пространства, обеспечивающего информационную поддержку принятия решений в сферах государственного контроля разработки, производства, поставки и эксплуатации авиационной техники (АТ) на основе данных о жизненном цикле изделий АТ, поступающих от субъектов ИАС МЛГ ВС: эксплуатантов ВС, организаций по техническому обслуживанию и ремонту АТ, поставщиков авиационного технического имущества и заводов-изготовителей АТ [1].

Оперативное взаимодействие и обмен информацией между субъектами ИАС МЛГ ВС осуществляется через интернет с помощью технического оператора ИАС МЛГ ВС – Информационно-аналитического центра (ИАЦ) ГосНИИ ГА (рис. 1), в функции которого входит:

- сопровождение сервера центральной базы данных (ЦБД) ИАС МЛГ ВС;
- предоставление интерфейсов доступа к данным;
- обеспечение достоверности данных и их защита при передаче, обработке и хранении.

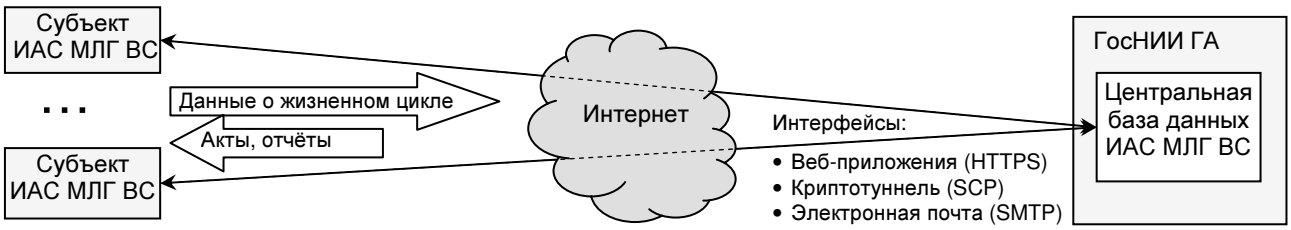

Рис. 1. Взаимодействие субъектов ИАС МЛГ ВС

Централизация хранения критичных для принятия решений об эксплуатации ВС данных и передача их через интернет сопряжены с угрозами сохранности и достоверности данных, что требует принятия комплекса мер по обеспечению их защиты.

Классификация возможных угроз и способов защиты

Субъектами ИАС МЛГ ВС являются как крупные авиазаводы, так и индивидуальные предприниматели-эксплуатанты авиации общего назначения. Значительный разброс в технической оснащённости, объёмах передаваемых данных и уровне владения информационными технологиями обуславливает разнообразие используемых в ИАС МЛГ ВС методов передачи данных, подверженным различным угрозам.

По используемым сетевым протоколам методы передачи данных в ИАС МЛГ ВС можно разделить на три группы:

1) **Веб-приложения**, размещённые на сайте ias.mlgvs.ru ("Учёт ресурсного состояния ВС", "Учёт ресурсного состояния компонентов ВС", "Сертификаты лётной годности", "Акты оценки аутентичности"), передающие данные по протоколу HTTP (англ. *HyperText Transfer Protocol* – "протокол передачи гипертекста").
2) **Обмен данными через криптотуннель** [2], основанный на протоколе SCP (англ. *Secure Copy* – "безопасное копирование"), с использованием в качестве транспортного протокола SSH (англ. *Secure SHell* – "безопасная оболочка").
3) **Электронная почта**, передаваемая по протоколу SMTP (англ. *Simple Mail Transfer Protocol* – простой протокол передачи почты).

Электронная почта, являясь наиболее доступным методом для пользователей, не владеющих информационными технологиями, имеет множество недостатков [3]. Их можно частично компенсировать с помощью дополнительного программного обеспечения (ПО) шифрования и электронной цифровой подписи (ЭЦП), но это нецелесообразно, так как делает передачу данных более сложной по сравнению с использованием других методов. Поэтому ИАЦ ГосНИИ ГА прилагает усилия по стимулированию пользователей к использованию альтернатив электронной почты. Например, эксплуатантам, отправляющим в ИАС МЛГ ВС данные технического состоянии компонентов ВС, предлагается вводить их в веб-приложении, предоставляющем полезный инструмент разноса наработок.

В табл. 1 приведены возможные угрозы данным, передаваемым через интернет и хранимым на серверах ИАС МЛГ ВС, а также способы противодействия этим угрозам.

Таблица 1

Типы угроз	Способы защиты данных
Перехват передаваемых данных	Шифрование интернет-трафика.
Злонамеренный ввод недостоверных данных	Авторизация пользователей. Защита от доступа в обход интерфейсов.
Злонамеренное удаление данных	Защита от доступа в обход интерфейсов.
Неправомерное извлечение данных	Авторизация пользователей. Защита от доступа в обход интерфейсов.
Потеря данных из-за сбоев и отказов	Построение отказоустойчивой системы. Резервное копирование.
Временный отказ в обслуживании	Построение отказоустойчивой системы.

В следующих разделах описаны особенности реализации используемых в ИАС МЛГ ВС способов защиты данных.

Шифрование интернет-трафика

Веб-приложения защищаются от перехвата и подмены трафика использованием расширения протокола HTTP, известного как HTTPS (англ. *HyperText Transfer Protocol Secure* – безопасный протокол передачи гипертекста). Трафик шифруется по алгоритму AES (англ. *Advanced Encryption Standard* – улучшенный стандарт шифрования) с использованием 256-битного ключа. В соответствии с протоколом HTTPS, подключаясь к серверу, браузер должен:

1) убедиться, что на запрос по доменному имени ias.mlgvs.ru отвечает сервер ГосНИИ ГА, а не подставной сервер злоумышленников, изменивших запись на ближайшем к пользователю сервере доменных имён (DNS);

2) безопасно передать серверу случайным образом сгенерированный для текущего сеанса ключ симметричного шифрования, которым сервер сможет дешифровать передаваемые данные.

Обе задачи решаются использованием SSL-сертификата, полученного ГосНИИ ГА от компании Thawte Inc., имеющей статус корневого удостоверяющего центра. Этот сертификат содержит открытый ключ сервера, которым браузер зашифровывает сеансовый ключ. Расшифровать сеансовый ключ (а, с его помощью, и передаваемые данные) можно только посредством парного закрытого ключа, который знает только сервер ГосНИИ ГА. Открытый ключ подписан ЭЦП компании Thawte Inc., сертификат которой предустановлен на всех компьютерах, что позволяет браузеру убедиться в подлинности сервера ГосНИИ ГА.

Обмен данными через криптотуннель, автоматизирующий передачу больших объёмов данных, обеспечивает шифрование всего трафика по алгоритмам AES с 256-битным ключом, которое является неотъемлемой составляющей используемого транспортного протокола SSH.

Для использования в авиакомпаниях, эксплуатирующие отечественные ВС в странах, подпадающих под ограничения США на экспорт средств криптографии, метод автоматического обмена через криптотуннель был доработан с целью использования дополнительного шифрования по ГОСТ 28147-89 с контролем целостности данных и идентификацией отправителя посредством ЭЦП по алгоритму ГОСТ Р 34.10-2001 [4].

Авторизация пользователей

Авторизация пользователей представляет собой процесс проверки прав на получение или отправку в ИАС МЛГ ВС определённой категории данных. Список прав доступа каждого пользователя хранится в базе данных ИАС МЛГ ВС.

Веб-приложения авторизуют пользователей по вводимому логину и паролю. Для предотвращения подбора пароля доступ к серверу блокируется несколько минут после пятой неудачной попытки авторизации. В целях повышения удобства пользования, все веб-приложения ИАС МЛГ ВС, включая Центральную нормативно-методическую библиотеку ГА, поддерживают сквозную авторизацию. Авторизованный в одном приложении пользователь идентифицируется другими приложения без ввода пароля по коду сессии, передаваемому с помощью технологии так называемых "cookie".

Сквозная авторизация не означает получения полного доступа ко всем приложениям. В каждом приложении любое обращение к данным предваряется идентификацией пользователя по коду сессии с проверкой прав доступа к конкретной категории данных, что также защищает от взлома путём подмены содержимого HTTP-запросов.

В процессе авторизации вместе с логином и паролем браузер передаёт серверу номера версий компонентов веб-приложения. Это позволяет с помощью описанного в [5] алгоритма предотвратить потерю данных в случае, когда разработчики меняют формат записей базы данных и обновляют код веб-приложения на сервере. Без принятия соответствующих мер браузер пользователя не сразу загружает обновлённый код, продолжая выполнять старый, сохранившийся в кэше браузера или прокси-сервера, и отправляя данные на сервер в старом, несовместимом формате.

Также, в процессе авторизации от браузера принимаются и сохраняются данные о версиях пользовательской операционной системе (ОС), прокси-сервера и конфигурации браузера, что упрощает локализацию проблем при оказании пользователям технической поддержки.

Обмен данными через криптотуннель для подтверждения подлинности пользователя использует 1024-битный ключ RSA, который передаётся субъекту ИАС МЛГ ВС в составе пакета клиентского ПО, обеспечивая более надёжную авторизацию пользователя по сравнению с использованием пароля. Встроенные в SSH-сервер средства защиты блокируют доступ в случае попыток перебора ключа авторизации. SSH-сервер сконфигурирован только для передачи файлов, функции терминального доступа и переназначения TCP-портов заблокированы.

Защита от несанкционированного доступа в обход интерфейсов

Центральная база данных ИАС МЛГ ВС, расположенная в локальной вычислительной сети (ЛВС) ИАЦ ГосНИИ ГА имеет два рубежа защиты от несанкционированного доступа к данным из интернета (рис. 2).

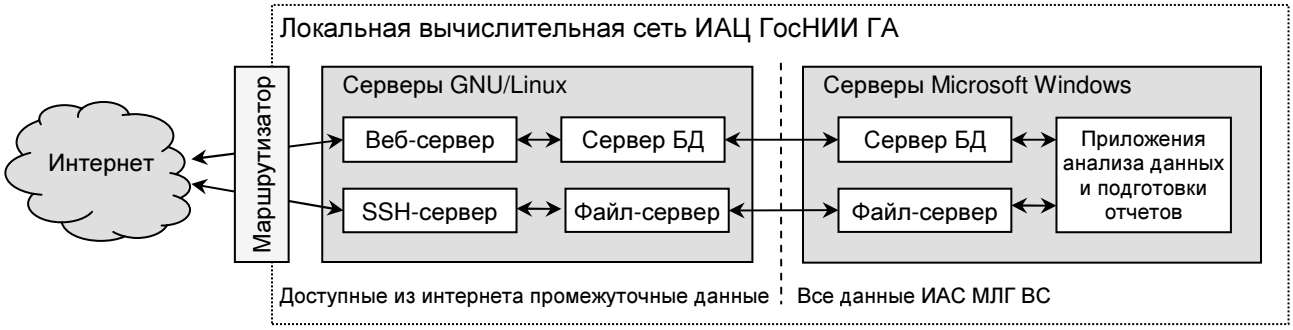

Рис. 2. Структура системы хранения и обработки данных ИАС МЛГ ВС

Внутренний рубеж защиты образуется разделением серверов ИАС МЛГ ВС на две группы:

1) Серверы, хранящие полный набор данных ИАС МЛГ ВС (базы данных, файловый архив фотографий пономерной документации компонентов ВС). Эти серверы, обрабатывающие данные и формирующие отчётную документацию, работают на ОС Microsoft Windows, используя такие преимущества платного ПО, как дружественный интерфейс, простота интеграции с корпоративными системами, наличие мастеров и конструкторов для быстрого решения прикладных задач.

2) Серверы интернет-интерфейсов (веб-приложений и обмена данными через криптотуннель), включая вспомогательные файл-сервер и сервер баз данных, используемые в качестве буфера для временного хранения ограниченного набора данных. Эта группа серверов работает под управлением ОС GNU/Linux, используя такие преимущества свободного ПО с открытым исходным кодом, как меньшая уязвимость к сетевым атакам, высокая стабильность и очень подробное журналирование ошибок и отладочной информации, необходимое для диагностики проблем, возникающих у удалённых пользователей.

Данные между двумя группами серверов передаются исключительно посредством выполняемых по расписанию программ-репликаторов, алгоритмы которых исключает возможность попадания произвольных данных из ЦБД в доступные через интернет серверы.

Внешний рубеж защиты создаётся маршрутизатором Cisco Systems, предоставляющим доступ из интернета только к рабочим портам веб- и SSH-серверов, и инспектирующим весь остальной трафик по технологии CBAC (Context-Based Access Control), блокируя любые входящие сетевые пакеты, не являющиеся ответами на исходящие из ЛВС запросы.

Построение отказоустойчивой системы хранения и обработки данных

Классическая серверная архитектура, при которой каждый физический сервер работает под управлением одной ОС с установленным набором приложений, не позволяет быстро восстановить работоспособность приложений в случае отказа сервера. Даже при наличии свободного запасного сервера, установка и конфигурирование ОС и приложений потребует нескольких часов. При этом оперативное восстановление данных не всегда возможно, например, в случае выхода из строя снятого с производства контроллера отказоустойчивого дискового массива.

Для предотвращения возможных потерь данных и многочасовых простоев в ИАЦ ГосНИИ ГА было решено модернизировать существующую серверную инфраструктуру [6], исключив

единую точку отказа и решив проблему быстрого переноса ОС с установленными приложениями с отказавшего сервера на резервный.

Одним из предлагаемых производителями серверов решений является использование блэйд-серверов (серверов-лезвий), размещённых в общем шасси и подключенных к общей дисковой системе хранения данных, что даёт возможность резервному серверу загрузиться из дискового раздела отказавшего сервера. Однако, проведённый анализ показал, что такая архитектура эффективна только при большом количестве однотипных серверов с равномерным распределением нагрузки, а ИАС МЛГ ВС построена вокруг высоконагруженного сервера баз данных, не поддающегося распараллеливанию на несколько физических серверов.

Решение было найдено в виртуализации серверов, обеспечивающей одновременную работу нескольких ОС (виртуальных машин) на одном физическом сервере (хосте). Для упрощения балансировки нагрузки все виртуальные машины были размещены на двух многоядерных серверах, производительности которых достаточно для обеспечения функционирования виртуальных машин, перенесенных с отказавшего хостов. Каждый физический сервер снабжен парой контроллеров, подключенных одновременно к двум двухпортовым контроллерам дисковой системы хранения данных IBM DS3512 (рис. 3).

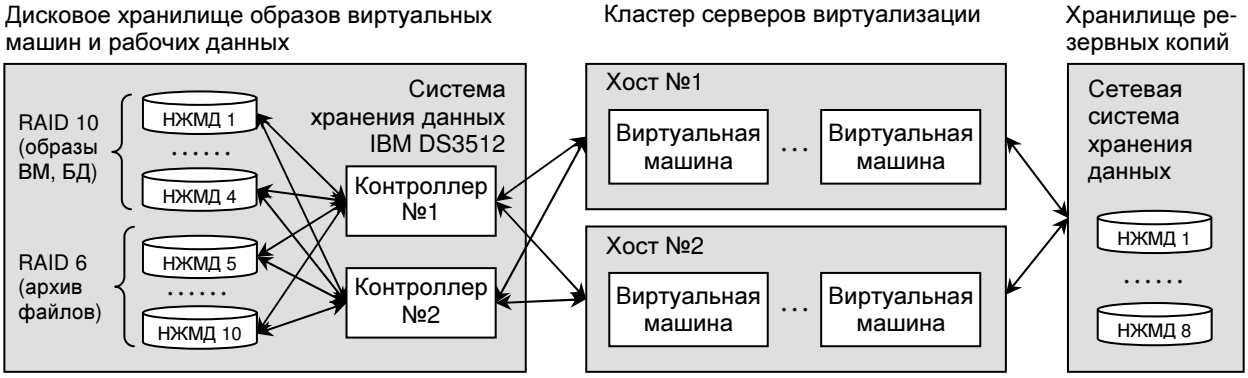

Рис. 3. Архитектура отказоустойчивого серверного кластера

В системе хранения используются высокоскоростные накопители на жестких магнитных дисках (НЖМД), каждый из которых оснащён двумя продублированными контроллерами SAS (Serial Attached SCSI). НЖМД объединены в отказоустойчивые дисковые массивы:

- RAID 10, обеспечивающий максимальное быстродействие – для хранения образов виртуальных машин и баз данных;
- RAID 6, обеспечивающий максимальную ёмкость при сохранении работоспособности в случае отказе двух НЖМД – для хранения файлового архива.

В результате было реализовано полное дублирование всего аппаратного обеспечения, что, наряду с поддержкой хостами виртуализации динамической многоканальной маршрутизации дискового хранилища, гарантирует сохранение работоспособности серверного кластера при отказе любого контроллера или нарушении контакта в любом разъёме.

Для оперативного устранения возможных сбоев физических серверов, они были снабжены контроллерами удалённого администрирования, позволяющими диагностировать и устранять проблемы на этапе загрузки ОС. Средства дистанционного управления дисковой системой хранения данных обеспечивают переназначение доступных серверам дисковых разделов, что в случае отказа сервера позволяет оперативно перенести его виртуальные машины и данные на другой сервер без физического копирования файлов.

Для предотвращения потерь данных вследствие ошибок программистов и администраторов, было настроено ежедневное автоматическое резервное копирование на сетевое хранилище данных (NAS), построенное на отказоустойчивом дисковом массиве.

Заключение

Виртуализация серверов ИАС МЛГ ВС на отказоустойчивом кластере позволила обеспечить надёжное хранение и бесперебойную обработку данных ИАС МЛГ ВС.

Реализованные в ИАС МЛГ ВС методы передачи данных через интернет с шифрованием трафика, авторизацией пользователей и выделением промежуточных серверов обеспечили приемлемый уровень защиты данных.

Имеющая множество недостатков электронная почта, остаётся для части пользователей единственным освоенным инструментом передачи данных. Для успешного внедрения более эффективных и безопасных методов информационного взаимодействия субъектов ИАС МЛГ ВС следует уделять внимание удобству использования пользовательских интерфейсов.

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. А.К. Благоразумов, И.Г. Кирпичев. Автоматизация информационного обмена в Информационно-аналитической системе мониторинга лётной годности воздушных судов // Научный вестник МГТУ ГА. – 2011. – №163. – С. 204–209.

3. А.К. Благоразумов, И.Г. Кирпичев. Способы передачи данных в Информационно-аналитическую систему мониторинга лётной годности воздушных судов через интернет // Научный вестник МГТУ ГА. – 2011. – №163. – С. 199-203.

4. А.К. Благоразумов, Ю.И. Евдокимов, И.Г. Кирпичев. Построение системы криптозащищённого обмена информацией о лётной годности воздушных судов // Научный вестник МГТУ ГА. – 2012. – №175. – С. 18 – 24.

5. И.Г. Кирпичев, А.К. Благоразумов. Обеспечение корректной работы веб-приложений в условиях кэширования // Научный вестник ГосНИИ ГА. – 2011. – №1. – С. 161–168.

6. А.К. Благоразумов, Г.Е. Глухов, И.Г. Кирпичев. Проблемы, решения технической реализации Информационно-аналитической системы мониторинга лётной годности воздушных судов // Научный вестник МГТУ ГА. – 2010. – №153. – С. 113 – 118.

PROTECTION OF DATA IN THE INFORMATION ANALYSIS SYSTEM FOR AIRCRAFT AIRWORTHINESS MONITORING

Kirpichev I.G., Blagorazumov A.K.

This article describes the methods used in The Information Analysis System for Aircraft Airworthiness Monitoring (IAS AAM) to protect data while transferring over the Internet as well as during data processing and storage in the database.

Keywords: IAS AAM, data exchange, encryption, fault tolerance, virtualization

Сведения об авторах

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.

Благоразумов Андрей Кириллович, 1970 г.р., окончил МАИ (1992), начальник группы Информационно-аналитического центра ГосНИИ ГА, автор 7 научных работ, область научных интересов – информационные технологии.