УДК 629.735.015:681.3

АВТОМАТИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА В ИАС МЛГ ВС

И.Г. КИРПИЧЕВ, А.К. БЛАГОРАЗУМОВ

Описывается метод автоматизации обмена данными Информационно-аналитической системы мониторинга лётной годности воздушных судов через Интернет, используя оригинальную технологию создания криптозащищённых каналов, не требующую перенастройки сетевого оборудования авиапредприятий.

Ключевые слова: лётная годность, ИАС МЛГ ВС, передача данных, обменные файлы.

Введение

Для функционирования Информационно-аналитической системы мониторинга лётной годности воздушных судов (ИАС МЛГВС) [1] необходим регулярный обмен данными между установленными в авиапредприятиях пользовательскими модулями (ПМ) и центральным программным модулем (ЦПМ), работающим в Информационно-аналитическом центре ГосНИИ ГА. Передача данных о лётной годности ВС через Интернет по цепочке неподконтрольных разработчикам ИАС МЛГВС Интернет-провайдеров является "узким местом" системы. В зависимости от отношения объема передаваемых данных к пропускной способности интернет-канала, длительность обмена может варьироваться от нескольких минут до нескольких часов. При такой длительности, согласно статистике веб-сайта обмена файлами ИАС МЛГ ВС (http://obmen.mlgvs.ru), обрывы связи фиксировались в 17% сеансов передачи данных.

Таким образом, осуществляемый вручную информационный обмен требует постоянного внимания со стороны оператора, которому приходится отслеживать обрывы связи и повторять передачу данных, оценивая их объём, чтобы сеанс завершился до окончания рабочего дня.

После того, как эксплуатация веб-сайта обмена показала, что большинство авиапредприятий может использовать Интернет для передачи данных ИАС МЛГ ВС, встала задача сделать следующий шаг – автоматизировать обмен, избавив оператора от выполнения рутинных операций и минимизировав влияние человеческого фактора на функционирование системы.

Как было показано в [2], передача данных сквозь защищающие локальные сети авиапредприятий межсетевые экраны является непростой задачей. Её можно решить двумя путями:

1) административным – согласовав с системными администраторами авиапредприятий, и, возможно их интернет-провайдерами, регламент о пропуске требуемого типа трафика, что обычно влечёт необходимость настройки сетевого оборудования.
2) техническим - разработав специальное программное обеспечение (ПО) передачи данных, использующее сетевые протоколы, не блокируемые межсетевыми экранами.

Поскольку информационный обмен необходимо настроить на множестве авиапредприятий, каждое из которых имеет свои особенности подключения к Интернету, универсальным и поддающимся тиражированию является только второй – технический путь.

Постановка задачи автоматизации обмена данными

Анализ задачи автоматизации информационного обмена в ИАС МЛГ ВС показал, что её решение разбивается на следующие этапы:

1) разработку технологии передачи данных сквозь межсетевые экраны без перенастройки сетевого оборудования;
2) разработку алгоритма информационного обмена;

3) реализацию разработанных технологии и алгоритма в программном коде.

Для каждого этапа были сформулированы соответствующие технические требования.

Технология передачи данных должна обеспечивать надёжное шифрование всех передаваемых данных на пути между ПМ субъекта ИАС МЛГ ВС и сервером ЦПМ ИАС МЛГ ВС.

Алгоритм информационного обмена должен обеспечивать:

- устойчивую к обрывам связи двустороннюю передачу данных;
- дистанционное обновление компонентов ИАС МЛГ ВС, в т.ч. кода ПО обмена;
- передачу на сервер журналов операций, необходимых для диагностики и отладки ПО.

Программный код подсистемы обмена должен, не "зависая", отрабатывать сбои и ошибки на всех уровнях сетевых протоколов. Это особенно актуально при передаче данных через множество промежуточных сетей посредством нескольких инкапсулированных (работающих один поверх другого) протоколов различных уровней (прикладного, представлений, сеансового, транспортного, сетевого, канального, физического) [3], так как, даже отлаженная коммуникационная программа (работающая на прикладном уровне) может потерять управляемость при возникновении коллизий сетевых пакетов на канальном уровне.

Технология передачи данных сквозь межсетевые экраны

При проведении анализа типов трафика, беспрепятственно пропускаемых сквозь межсетевые экраны большинства организаций [2], было отмечено, что протокол HTTPS (англ. ***H**yper**T**ext **T**ransfer **P**rotocol **S**ecure* – "протокол передачи гипертекста, использующий шифрование"), пропускается всем сетевыми устройствами (в т.ч. прокси-серверами) без вмешательства в передаваемые данные, так как любое изменение зашифрованных данных приводит к невозможности их расшифровки.

Поскольку стояла задача обеспечения передачи данных именно в зашифрованном виде, для беспрепятственного прохождения сквозь любые системы защиты сетей достаточно имитировать HTTPS-трафик. Как следовало из теории и было подтверждено экспериментами, не имея возможности проинспектировать зашифрованный трафик, сетевые устройства опознают использования протокола HTTPS по номеру TCP-порта сервера (HTTPS использует порт 443).

Выбор транспортного протокола, использующего шифрование и требующего только одного открытого на сервере TCP-порта, был очевиден – этим условиям удовлетворяет протокол SSH (англ. ***S**ecure **SH**ell* – "безопасная оболочка"). Он создаёт крипто-каналы и туннелирует в них любые сетевые протоколы, в т.ч. протоколы передачи файлов. Надёжность алгоритмов шифрования и их реализации в SSH доказана временем – SSH уже 15 лет является основным средством удалённого доступа к серверам на операционных системах (ОС) семейства UNIX.

Схема туннелирования трафика информационного обмена приведена на рис. 1.

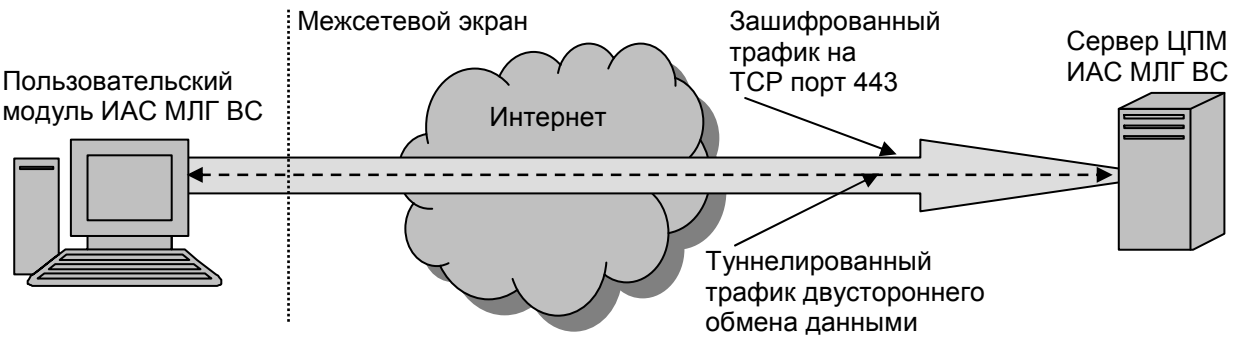

Рис. 1. Туннелирование трафика

Для работы в составе ПМ ИАС МЛГ ВС был выбран свободно распространяемый SSH-клиент для ОС Windows под названием "Putty". Имея графический интерфейс для конфигурирования сетевых настроек, он может управляться из командной строки, что облегчает его интеграцию с другим ПО.

Алгоритм информационного обмена

Для обеспечения устойчивости к обрывам связи, данные передаются пакетами, размер которых выбирается таким, чтобы время передачи пакета не превышало десятка минут. Пакеты формируются упаковкой передаваемых файлов в многотомный архив с помощью свободно распространяемого мультиплатформенного архиватора 7-Zip.

Для ИАС МЛГ ВС критична последовательность получаемых данных, так как более свежие обменные файлы могут содержать обновления предыдущих файлов. Потери пакетов необходимо своевременно обнаруживать, для сохранения порядка передачи оставшихся пакетов. Обнаружение потерь было реализовано сравнением размера отправленного и полученного файла, а обеспечение порядка передачи – путём именования файлов по дате создания, что позволило задавать порядок простой сортировкой по алфавиту. Тома архива дополняются файлом, содержащим общее количество томов. Его получение принимающей стороной служит сигналом о готовности всех томов архива к распаковке.

Временная диаграмма процесса обмена данными изображена на рис. 2. Для краткости и удобства восприятия описание алгоритма приведено в терминологии клиент-сервер, где под клиентом понимается рабочая станция ПМ ИАС МЛГ ВС или, в зависимости от контекста, управляющее обменом ПО, а под сервером – ЦПМ ИАС МЛГ ВС.

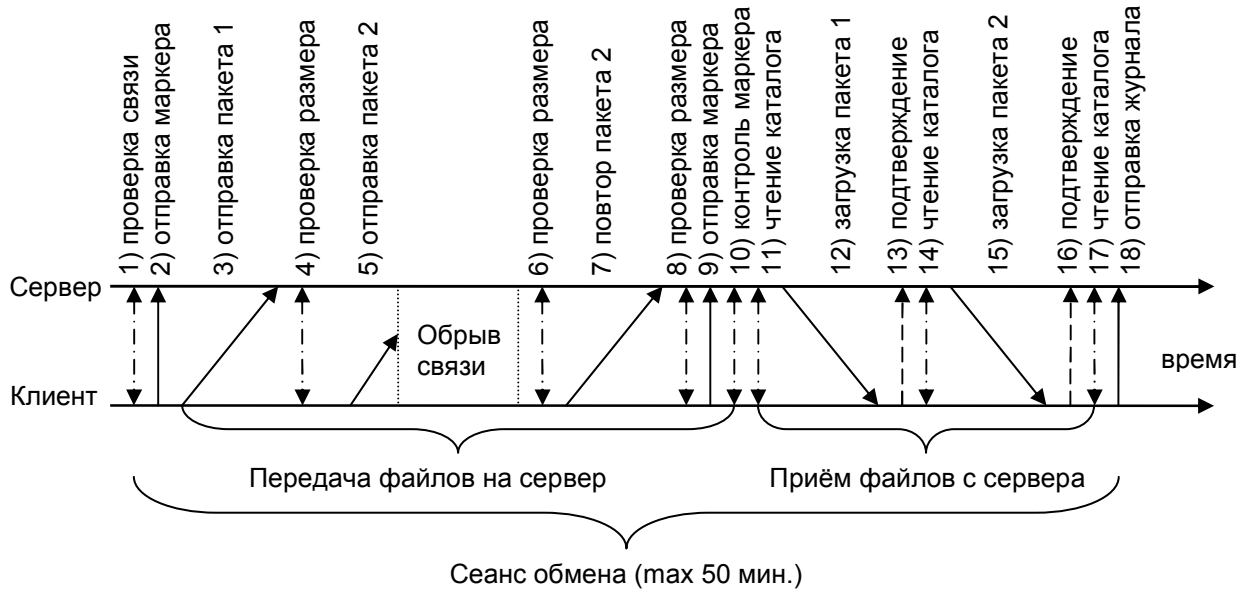

Рис. 2. Временная диаграмма обмена между ПМ и сервером ЦПИ ИАС МЛГ ВС

Сеанс начинается с проверки связи между клиентом и сервером командой чтения серверной папки пользователя (этап 1). При отсутствии связи программа ожидает две минуты и повторяет проверку. При удачном соединении проверяется наличие на сервере необходимых папок (входящих, исходящих файлов, и журналов обмена).

В начале каждого сеанса связи на сервер отправляется маркер – файл, содержащий текущую дату и версию клиентского ПО. Он свидетельствует о работоспособности клиента в отсутствии передаваемых данных, что актуально при обновлении клиентского ПО.

Пакеты передаются на сервер поочерёдно, в алфавитном порядке (этап 3). Отправка завершается запросом с сервера и сравнением размера принятого файла пакета (этап 4). Если, к примеру, на этапе 5 связь оборвалась, то при несовпадении размера (этап 6) отправка второго пакета будет повторена (этап 7).

После отправки последнего тома клиент передаёт на сервер файл-маркер конца архива (этап 9). Получив его, сервер распакует файлы и отдаст на обработку в ЦПМ ИАС МЛГ ВС.

Приём файлов начинается чтением каталога загружаемых файлов (этап 11). В целях упрощения программного обеспечения и из соображений безопасности, для передачи файлов используется простой протокол SCP, не поддерживающий удаление файлов на сервере. Задача удаления скачанных пакетов с сервера решается отправкой подтверждений – файлов с именами, соответствующими файлам пакетов (этапы 13, 16). Выбирая очередной пакет для скачивания, клиент пропускает подтверждённые пакеты, а периодически запускаемая на сервере программа удаляет их и файлы подтверждений.

После отправки и скачивания всех файлов, клиент проверяет возраст журналов операций, и, если он превышает заданный порог, архивирует и отправляет журналы на сервер. Эти журналы выполняют функцию обратной связи, необходимой для отладки ПО.

Скорости передачи данных через Интернет-канал в обе стороны могут различаться, особенно при возникновении проблем с маршрутизацией. Для устранения вызываемых ассимметрией проблем (например, задержки отправки данных из-за падения скорости приёма) алгоритмом предопределяется, что сеансы поочерёдно начинаются приёмом данных или их отправкой.

Реализация самообновления программного кода

Для ПО информационного обмена не составляет проблем получать с сервера и устанавливать обновления программного кода ИАС МЛГ ВС. Однако, обновление собственного кода, устанавливающего связь и загружающего файлы, имеет две особенности:

1) ОС может блокировать выполняемый код от модификации;
2) инициация соединений именно клиентом приводит к тому, что допущенные в коде ПО ошибки, которые препятствуют загрузке файлов, уже невозможно исправить без непосредственного доступа к рабочей станции ПМ ИАС МЛГ ВС.

Для избавления от этих проблем было найдено простое и изящное решение, заключающееся в дублировании реализующего алгоритм обмена программного кода, крипто-ключей и сетевых настроек. Копии программ обмена запускаются по очереди, через день, и наделёны способностью обновления только своего дублёра (см. рис. 3).

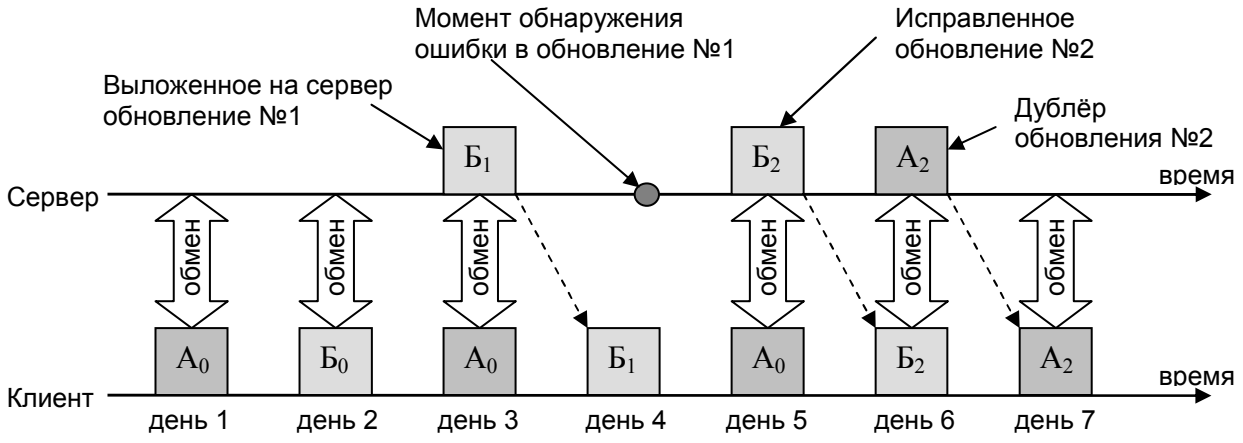

Рис. 3. Временная диаграмма процесса самообновления

На рисунке дублирующие друг-друга компоненты (далее для краткости называемые "программами") обозначены буквами А и Б, а их версии – цифровыми индексами. Предположим, что в третий день на сервер было выложено обновление $Б_1$, которое было скачано и установлено программой $А_0$. Если в следующий день программа $Б_1$ из-за ошибки в коде не сможет выйти на связь, это обнаружится по отсутствию маркеров сеансов и будет исправлено в обновлении $Б_2$. В пятый день программа $А_0$ скачает и установит обновление $Б_2$. В шестой день, убедившись в работоспособности второй версии обновления, администратор выложит на сервер дублёра – $А_2$, который будет скачан и установлен в этот же день вместо программы $А_0$. Во все последующие дни, до следующих обновлений, поочерёдно будут запускаться программы $А_2$ и $Б_2$.

Программная реализация информационного обмена

Помимо выполняющего транспортные функции пакета ПО Putty, в составе ПМ ИАС МЛГ ВС должна выполняться управляющая программа, реализующая алгоритм обмена. К языку программирования управляющей программы были предъявлены два требования:

1) наличие развитых средств обработки текста (коммуникационное ПО выводит результаты выполнения команд отформатированными для лучшего восприятия людьми);
2) удобство инспектирования программного кода лицами, ответственными за соблюдение информационной безопасности на местах, поскольку ПО передаёт зашифрованную информацию за пределы локальной сети.

Всем этим требованиям удовлетворяет язык Perl [4]. Он принадлежит к классу скриптовых языков, т.е. программы существуют исключительно в виде открытого текста, выполняемого построчно интерпретатором. Интерпретатор Perl реализован для всех операционных систем, его версия для ОС Windows состоит всего из двух не требующих инсталляции файлов.

Пробная эксплуатация коммуникационных программ показала их хорошую устойчивость к обрывам связи. Во всех случаях управление своевременно возвращалось в управляющую программу. Принимая во внимание, что ответственность за бесперебойный обмен лежит на ПМ ИАС МЛГ ВС, для достижения безупречной стабильности было решено добавить функцию "сторожевого таймера". Суть её в том, что управляющая программа запускается каждый час из планировщика заданий ОС Windows, установленого на принудительное завершение задания через пятьдесят минут после запуска. Управляющая программа вычисляет максимальное время передачи пакетов в каждом направлении и не начинает передачу, если пакет не успевает передаться к наступлению пятидесятой минуты. Если по истечении отведённого времени программа не завершиться самостоятельно, её прервёт операционная система. В этом случае, на гарантированное завершение всех дочерних процессов отводится защитный десятиминутный интервал.

Заключение

Предложенный метод информационного обмена был реализован на практике в ряде субъектов ГА, среди которых:

- Федеральное агентство воздушного транспорта (Росавиация);
- Приобское межрегиональное территориальное управление воздушного транспорта;
- Красноярское межрегиональное территориальное управление воздушного транспорта;
- ОАО "Пермский моторный завод";
- Ульяновское самолётостроительное предприятие ЗАО "Авиастар-СП";
- ЗАО "Иркутский центр сертификации экземпляра воздушного судна "Эксперт-Профи";
- ООО "Тюменский центр по сертификации объектов гражданской авиации "Аудит-Эйр";
- АНО "Красноярский межрегиональный центр авиационной сертификации".

Опытная эксплуатации ПО информационного обмена ИАС МЛГ ВС в разных регионах РФ показала эффективность и обоснованность выбранных решений. Вместе с тем, выявлена про-

блема в одной организации, где пароль от доступа к Интернету через прокси-сервер ежемесячно менялся – в этом случае потребовалось после кажой смены пароля менять его и в настройках коммуникационного ПО.

Разработанные в рамках совершенствования ИАС МЛГ ВС метод автоматизации информационного обмена и оригинальный способ передачи данных сквозь межсетевые экраны, могут найти применение для решения подобных задач в любых информационных системах.

Дальнейшее улучшение алгоритма обмена возможно по пути добавления функции адаптивного определения размера передаваемого пакета, что позволит лучше задействовать пропускную способность физического канала связи без необходимости ручной настройки ПО.

ЛИТЕРАТУРА

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

2. И.Г. Кирпичев, А.К. Благоразумов. Способы передачи данных в ИАС МЛГ ВС через Интернет – Научный вестник МГТУ ГА, серия Аэромеханика, прочность, лётная годность, № <готовящийся к печати номер, в который отправлена указанная статья>.

3. Дуглас Камер. Сети TCP/IP, том 1. Принципы, протоколы и структура – М.: Вильямс, 2003 – С. 880.

4. Уолл Л., Кристиансен Т., Орвант Д. Программирование на Perl – СПб: Символ-Плюс, 2004. – С. 1152

AUTOMATION OF DATA EXCHANGE IN THE INFORMATION ANALYSIS SYSTEM FOR AIRCRAFT AIRWORTHINESS MONITORING

Kirpichev I.G., Blagorazumov A.K.

The article describes how to automate data exchange via the Internet in the Information Analysis System for Aircraft Airworthiness Monitoring using crypto-channels without necessity of mediate networks' equipment reconfiguration.

Keywords: airworthiness, information system, data exchange.

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 3-х монографий и более 30-ти 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 4-х научных работ, область научных интересов – информационные технологии.