УДК 629.735.015:681.3

СПОСОБЫ ПЕРЕДАЧИ ДАННЫХ В ИАС МЛГ ВС ЧЕРЕЗ ИНТЕРНЕТ

И.Г. КИРПИЧЕВ, А.К. БЛАГОРАЗУМОВ

Приведён анализ возможных способов передачи данных в Информационно-аналитическую систему мониторинга лётной годности ВС через Интернет с оценкой отношения эффективности к простоте реализации.

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

Введение

Эффективность и качество деятельности по сопровождению эксплуатации авиационной техники (АТ) могут быть значительно повышены применением информационных систем, автоматизирующих анализ информационных потоков о процессах эксплуатации АТ. Однако, максимальная отдача от их внедрения может быть достигнута, лишь когда информационные системы субъектов ГА оперативно обмениваются актуальными данными о жизненном цикле воздушных судов и их компонентов. Разработанная в Информационно-аналитическом центре (ИАЦ) ГосНИИ ГА Информационно-аналитическая система мониторинга лётной годности воздушных судов (ИАС МЛГВС) [1] требует передачи относительно больших объёмов файлов, содержащих фотокопии пономерной документации компонентов ВС.

Среди доступных большинству организаций способов оперативной передачи данных сегодня нет альтернативы Интернету, являющемуся совокупностью независимых сетей, объединенных маршрутизаторами и фильтрующими трафик межсетевыми экранами (называемыми также "брандмауэрами" или "файерволами"). За сорок лет существования Интернета было разработано множество сетевых протоколов, оптимизированных для передачи различных типов данных.

В настоящее время наблюдается тенденция к усилению фильтрации и блокировки трафика, являющаяся защитной реакцией на постоянно растущие угрозы в виде вирусов, сетевых червей, хакерских атак, а также перегружающий сетевое оборудование трафик файлообменных сетей и засоряющую электронную почту рекламу ("спам").

Дополнительные искусственные ограничения возникают из-за того, что российские Интернет-провайдеры практически не предлагают безлимитные тарифы для юридических лиц, взимая оплату, пропорциональную объёму переданных данных. Проблема заключается даже не в стоимости трафика, а в намеренном блокировании межсетевыми экранами большинства организаций сетевых протоколов, оптимизированные для передачи объёмных файлов. Это обусловлено тем, что большие размеры свойственны, в первую очередь, развлекательным аудио- и видеофайлам, в передаче которых нет производственной необходимости.

В связи с вышеизложенным, для эффективного функционирования ИАС МЛГ ВС требуется выбрать способ передачи больших объёмом данных посредством сетевых протоколов, изначально не предназначенных для передачи больших файлов, но неблокируемые межсетевыми экранами авиапредприятий. Альтернатива в виде перенастройки межсетевых экранов не является приемлемой для многих авиапредприятий по следующим причинам:

- заинтересованным в информационном обмене лицам не всегда удаётся убедить системных администраторов произвести действия, ослабляющую отлаженную защиту сетей;
- системные администраторы, установив межсетевой экран с настройками по-умолчанию, могут не обладать квалификацией, достаточной для внесения требуемых изменений;
- может потребоваться настройка оборудования, не принадлежащего авиапредприятию.

Характеристика данных, передаваемых в ИАС МЛГ ВС

ИАС МЛГ ВС состоит из центрального программного модуля (ЦПМ), развёрнутого на серверах ИАЦ ГосНИИ ГА, и пользовательских модулей (ПМ), устанавливленных на рабочих станциях субъектов ГА. Часть авиапредприятий в поседневной деятельности пользуются другими информационными системами, экспортируя из них данные для передачи в ЦПМ ИАС МЛГ ВС. В обоих случаях, на сервер ЦПМ ИАС МЛГ ВС периодически передаются:

- структурированные текстовые файлы, содержащие обновления базы данных о жизненном цикле воздушных судов и их компонентов (так называемые "обменные файлы");
- фотокопии пономерной документации компонентов ВС.

Для удобства передачи файлы упаковываются в архив, большая часть которого приходится на графические файлы.

Для каждого авиапредприятия объём передаваемых данных и периодичность их отправки напрямую зависит от количества и типа обслуживаемых ВС. По накопленной статистике, в среднем авиапредприятие отправляет по 50Мбайт два раза в месяц, максимальный объём файла составил 1300Мбайт, а максимальный суммарный за месяц – 2300Мбайт.

Анализ существующих способов передачи данных

При анализе доступных сетевых протоколов использовалась модель подключения локальной сети (рис. 1) типичная для организаций с количеством рабочих мест более десяти. При этом для рабочей станции гарантированно разрешены только следующие сетевые протоколы:

- SMTP (электронная почта);
- HTTP (просмотр веб-сайтов);
- HTTPS (полезен нестандартной возможностью использования в качестве транспорта для VPN-туннеля к серверу, по котором уже можно копировать файлы напрямую);
- трафик сети Skype (не будучи разрешенным, он просто не может быть заблокирован известными средствами);

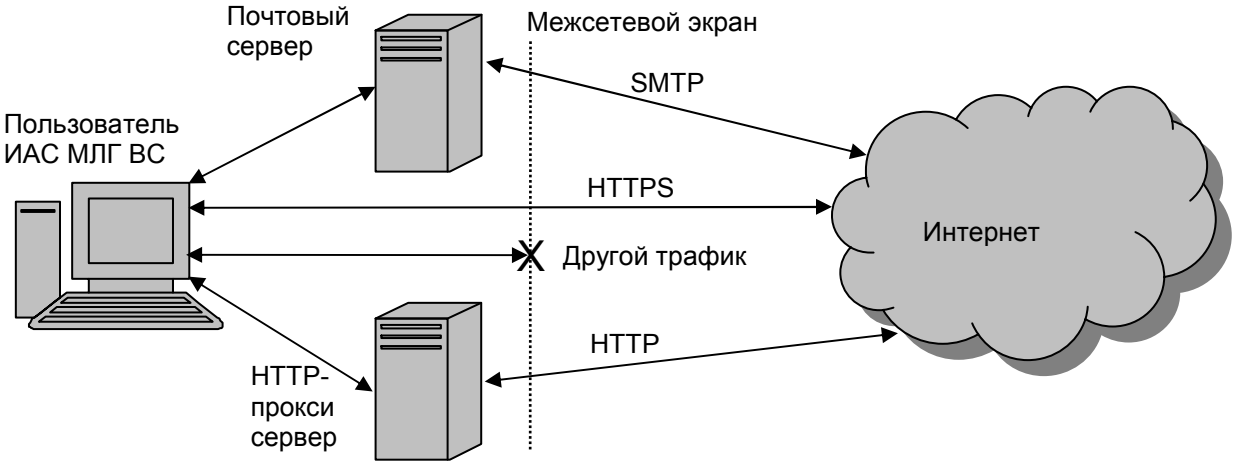

Рис. 1. Фильтрация трафика в типовой локальной сети

Электронная почта доступна в каждой организации, имеющей доступ в Интернет. Её использование для передачи больших файлов имеет следующие недостатки:

- Объём одного почтового сообщения ограничен единицами, реже - десятками мегабайт. Точная величина зависит от настроек конкретных почтовых серверов, из-за чего для гарантиро-

ванной доставки приходится делить отправляемые данные ИС МЛГ ВС в среднем на 7 сообщений (был случай, когда отправитель разделил файл на 236 частей), что крайне нетехнологично как при отправке, так и при получении.

- Для борьбы со "спамом" почтовый трафик подвергается фильтрации. Многие почтовые серверы используют зарубежные черные списки, часто блокирующие даже крупнейших российских Интернет-провайдеров, обслуживающих десятки тысяч пользователей. Успешная доставка почта сегодня не может гарантировать её доставку завтра.

- Почтовый сервер может отказать в приёме сообщений из-за переполнения "почтового ящика" пользователя, или другой внутренней ошибке. Уведомления отправителя об ошибках могут быть отключены, чтобы не дать рассыльщикам "спама" обнаружить действующие адреса электронной почты. В итоге, потеря данных может остаться незамеченной.

- Случается, что современные протоколы авторизации блокируются маршрутизаторами с включеным режимом инспектирования почтового трафика. При этом доставка сообщений невозможна, если на сервере корреспондента устаревшие протоколы отключены в целях защиты от "спама".

- Для совместимости с серверными программами 30-ти летней давности, передаваемые файлы до сих пор кодируются набором печатных символов, из-за чего полезный объём информации составляет менее 75% от передаваемого.

Эти недостатки позволяют сделать вывод о низкой эффективности электронной почты для передачи данных в ЦПМ ИАС МЛГ ВС, не оправдывающей простоту её использования.

HTTP (англ. ***H**yper**T**ext **T**ransfer **P**rotocol* – "протокол передачи гипертекста"). Служит транспортом при просмотре веб-сайтов. Начиная с версии 1.0, принятой в 1995г., протокол дополнен возможностью отправлять на сервер произвольные данные. Отправка файлов возможна при подключении к специально разработанному веб-сайту.

Анализ статистики веб-сервера ИАЦ ГосНИИ ГА (www.mlgvs.ru) показал, что в 37% авиапредприятий веб-трафик пропускается через прокси-сервер, установленный в целях:

- учёта потребления трафика отдельными пользователями;
- блокирования конкретных сайтов (как правило, социальных сетей) или небезопасного содержимого веб-страниц;
- снижения потребляемого трафика за счет кэширования ранее скачанных файлов.

Практически, прокси-сервер создаёт препятствия передаче данных из-за:

- устанавливаемых местными системными администраторами произвольных ограничений на длину передаваемого файла, что не позволяет гарантированно передавать большие файлы без разбиения их на части;
- устанавливаемых ограничений на длительность открытой сессии, что также ограничивает длину передаваемого файла величиной, непредсказуемой из-за зависимости от скорости всей цепочки задействованных Интернет-каналов;
- кэширования ответов веб-сервера (подмены актуальных данных ранее сохранёнными).

Использование веб-трафика привлекательно прежде все тем, что отправка файлов возможна с любого компьютера, имеющего выход в Интернет, а от пользователя требуется минимум навыков – достаточно только открыть Интернет-браузер, ввести адрес соответствующего веб-сайта и следовать отображаемым указаниям. В отличие от электронной почты, файлы передаются без помощи промежуточных серверов, а подтверждение доставки файла можно получить немедленно. Большинство создаваемых прокси-серверами проблем можно обойти, приняв специальные меры при разработке серверного программного обеспечения (ПО), однако, накладываемые ограничения на размер передаваемого файла всё же заставляют пользователя передавать большие объёмы данных частями.

В итоге можно сделать вывод, что применение веб-трафика для передачи данных ИАС МЛГ ВС достаточно эффективно и несложно реализуемо.

HTTPS (англ. **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure) – расширение протокола HTTP, поддерживающее шифрование. Этот протоко не блокируется межсетевыми экранами, поскольку служит базовым для веб-сайтов, требующих безопасного соединения (платёжные системы, «личные кабинеты» операторов связи, серверы электронной почты). Возможность передавать любые данные в зашифрованном виде через межсетевые экраны используется для туннелирования в HTTPS других сетевых протоколов. Наибольший интерес представляет технология VPN (англ. **V**irtual **P**rivate **N**etwork – "виртуальная частная сеть"), работающая поверх протокола HTTPS.

Суть технологии VPN заключается в объединении двух и более компьютеров, находящихся в разных физических сетях в одну логическую сеть [2]. При этом вся информация по физическим сетям передаётся в зашифрованном виде. После установки VPN-соединения файлы можно копировать с компьютера на сервер средствами операционной системы или сторонними файловыми менеджерами так, как если бы компьютер и сервер находились внутри одной локальной сети.

Следует особо подчеркнуть, что технология VPN имеет массу разновидностей, одна только классификация которых занимает несколько страниц, а способностью работать сквозь межсетевые экраны обладает только VPN поверх HTTPS, реализуемый пакетом ПО OpenVPN [3], который требует весьма квалифицированной настройки как на стороне рабочей станции, так и на стороне сервера. Встроенный же в ОС Windows легко настраиваемый VPN-клиент не может работать ни через прокси-серверы, ни без поддержки Интернет-провайдером протокола GRE (англ. *Generic Routing Encapsulation* – "общая инкапсуляция маршрутов"), ни в случаях, когда VPN уже используется для подключения к самому Интернет-провайдеру.

Недостатком объединения компьютеров разных организаций посредством VPN является возможность беспрепятственного проникновения сетевых вирусов из одной организации в другую, если не приняты специальные меры по защите каждого компьютера.

Поскольку внутри VPN-туннелей для копирования файлов используются файловые менеджеры, предназначенные для локальных сетей, в которых обрывы связи являются нештатной ситуацией, автоматическое продолжение копирование файла с места обрыва не поддерживается. Контроль за обрывами связи и повтор копирования возлагается на оператора, что снижает эффективность этого способа передачи данных.

К тому же, сложность развёртывания VPN поверх HTTPS на стороне клиента не позволяет использовать эту технологию во всех авиапредприятиях, в которых требуется обеспечить передачу данных в ЦПМ ИАС МЛГ ВС.

Сеть Skype разработана в 2003 году для передачи голоса через Интернет, и в данный момент насчитывает более 100 миллионов пользователей, из которых одновременно подключены к сети 15-20 миллионов. С технической точки зрения, Skype является идеальной транспортной сетью, обеспечивая двусторонний обмен данными между любыми подключёнными к Интернету компьютерами. Её трафик успешно проходит через любые межсетевые экраны, благодаря способностям использовать нетрадиционным способом все разрешенные сетевые протоколы и задействовать чужие компьютеры в качестве "перевалочного пункта" [4]. Клиент сети Skype предоставляет программный интерфейс, позволяющий сторонним приложениям передавать файлы.

Однако главным недостатком, перечёркивающим все преимущества Skype, является полная закрытость его сетевого клиента. Весь исполняемый код зашифрован и снабжён средствами противодействия программам-отладчикам, а передаваемый трафик тщательно шифруется. Поскольку Skype способен обходить все системы защиты локальной сети, вынося за её пределы любую информацию, его использование в организациях может быть запрещено по соображениям безопасности, что не позволят рекомендовать этот способ передачи данных пользователям ИАС МЛГ ВС.

Выводы

Среди всех доступных способов передачи данных в ЦПМ ИАС МЛГ ВС посредством Интернета, самым оптимальным по отношению эффективности к простоте использования оказался обмен данными через веб-сайт по протоколу HTTP.

Для реализации этого способа на практике был разработан сервис обмена данными ИАС МЛГ ВС (http://obmen.mlgvs.ru). Для решения проблем обрыва связи, возникавших в среднем в 17% сеансов отправки данных, было разработано специальное ПО упаковки фотографий. Оно помещает файлы в многотомные архивы, предварительно обрабатывая фотографии, уменьшая их объём за счёт избыточного разрешение и корректируя контрастность изображений.

Хотя веб-сайт обмена данными не является идеальным средством информационного обмена, его эксплуатация показала, что пропускная способность Интернет-каналов большинства авиапредприятий удовлетворяет требованиям к обмену данными ИАС МЛГ ВС, а накопленная сайтом статистика обеспечила разработчиков достоверными данными, позволившими научно обоснованно приступить к решению следующей задачи – автоматизации информационного обмена в ИАС МЛГ ВС.

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. Олег Колесников, Брайан Хетч. Linux. Создание виртуальных частных сетей (VPN). – М.: КУДИЦ-Образ, 2004 – 464 с.

3. Алексей Коршунов. OpenVPN: доступ повышенной проходимости // Системный администратор – М., 2007 – №7 – С.53-59

4. Крис Касперски. Skype – скрытая угроза // Хакер – М., 2007 – №4(100) – С. 64-69

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

Kirpichev I.G., Blagorazumov A.K.

The article contains analysis of possible methods to send data to the Information Analysis System for Aircraft Airworthiness Monitoring with assessments of efficiency and simplicity each method provides.

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.