Рассмотрены примеры решения задач моделирования на ЭВМ и многокритериальной оптимизации систем передачи непрерывных сообщений цифровыми методами. При этом путем статистических испытаний получены семейства зависимостей погрешности передачи сообщений от соотношения сигнал/шум при использовании разных видов модуляции. Оценивание эффективности и оптимизация цифровых систем передачи непрерывных сообщений выполнялось по совокупности показателей качества: энергетической, частотной, информационной эффективности и погрешности передачи сообщений. Для сформированного множества допустимых вариантов системы получены оценки значений показателей качества, выполнен дискретный выбор подмножества Парето-оптимальных систем и построены многомерные диаграммы обмена показателей качества систем. Затем введен результирующий скалярный показатель качества и выбран единственный вариант системы. В приведенных примерах решения задач моделирования и оптимизации систем связи полагалось, что математической моделью передаваемых сообщений служил гауссовский случайный сигнал с разным видом корреляционной функции; для передачи использовались разные виды модуляции (амплитудная, частотная, фазовая); в канале связи действовал гауссовский белый шум; на приемной стороне применялись когерентные и некогерентные методы обработки принимаемых сигналов.

Литература

1. Захарченко М.В., Стеклов В.К., Князева Н.О. и др. Автоматизація проектування пристроїв, систем та мереж зв"язку.- К.: Радіоаматор, 1996.
2. Алексеев О.В., Головкин А.А., Пивоваров И.Ю. Автоматизация проектирования радиоэлектронных средств. - М.: Высшая школа, 2000.

— ◙ —

Использование защищенной почты для ДО

Горбенко И.Д., Качко Е.Г., Марченко С.Ю., Дягилева Ф.Г.
Харьковский национальный университет радиоэлектроники,
Институт информационных технологий,
Харьков, Украина,
E-mail: kachko@univer.kharkov.ua

Abstract

The questions of the protected mail use for remote education are considered. The application of the digital signature will ensure integrity, authenticity and participation for all documents of the email. The digital signature law on the will give legal force to the documents

Дистанционное образование используется в настоящее время достаточно широко. Лицам, которые обучаются, предоставляется возможность изучения предметов по специально разработанным электронным учебникам. Они могут

выполнять практические и лабораторные работы по методическим указаниям, разработанным для дистанционного обучения. Выполненные контрольные работы отсылаются с использованием электронной почты. Электронная почта, как и обычная почта, недостаточно надежна. Более того, если целостность конверта видна на глаз, то сообщение может быть искажено, аннулировано, или подложено сообщение, которое пользователь не посылал. В этом случае ни отправитель не может быть убежден, что посланное им сообщение доставлено адресату, если даже пришло соответствующее уведомление, ни получатель не может быть уверен, что он получил то письмо, которое ему отправляли. Для обеспечения целостности, подлинности и причастности отправляемых и получаемых сообщений вместо обычной электронной почты целесообразно использовать защищенную почту. В данном докладе рассматриваются принципы построения и использования защищенной почты для дистанционного образования.

Что необходимо защищать? Прежде всего, необходимо обеспечить целостность и подлинность сообщений. Например, пусть слушатель прислал контрольную работу, в которой допущены грубые ошибки. Преподаватель не зачел данную контрольную работу. Обучаемый заявляет, что он присылал контрольную работу другую, в которой указанных ошибок не было. В этом случае ни обучаемый, ни преподаватель не могут доказать свою правоту, если не используется цифровая подпись для электронной почты. Более того, преподаватель может сказать, что такой контрольной он вообще не получал, или получил ее после требуемого срока. Все это можно "доказать", подложив в требуемые папки необходимые письма с требуемой датой. Примеры можно бесконечно продолжать. Для исключения подобных недоразумений цифровая подпись под документами необходима. Кроме того, как и любой вид работы, консультации преподавателей для дистанционного образования должны оплачиваться. Как регистрировать эти консультации? Для этих целей можно использовать обычные журналы, но в этом случае обучаемый, неудовлетворенный результатами экзамена, может заявить об отсутствии консультаций. Если консультации проводились в виде электронных писем в рамках защищенной почты, они хранятся как защищенные сообщения, автоматически регистрируются в журналах с цифровой подписью и не могут быть изменены на обоих концах канала связи. В случае принятия закона о цифровой подписи, такие журналы могут использоваться в качестве обоснования необходимости оплаты консультаций, так как имеют юридическую силу. Перечень дополнительных возможностей, обеспечиваемых цифровой подписью, может быть продолжен.

Рассмотрим, как использовать защищенную электронную почту.

Существующие программы, которые называются почтовыми клиентами и используются для отправки и приема электронной почты, имеют встроенные средства защиты. Эти средства позволяют выполнять криптографические операции, в том числе, цифровую подпись. Но стандартные средства формируют цифровую подпись не по стандартам Украины, потому не могут использоваться для работы с документами, имеющими юридическую силу, поэтому мы предлагаем собственную систему защищенной почты.

Определены функциональные требования к системе защиты информации для электронной почты, требования к интерфейсу и среде, в которой она функционирует. При определении функциональных требований учтены стандартные услуги, которые должны поставляться системами защиты с учетом требований использования национальных Стандартов на криптографию. При определении требований к пользовательскому интерфейсу учтено, что электронную почту могут использовать неподготовленные пользователи, поэтому, чем интерфейс проще, тем шире сможет использоваться система, тем меньше вероятность ошибок. При определении требований к окружению мы рассмотрели основные почтовые программы и наиболее распространенные почтовые серверы и в требованиях заложена возможность использования этих программ с наиболее полным покрытием их режимов функционирования. Для поддержки интернет - технологий используются различные операционные системы, в том числе Windows, различные версии Unix. Окончательная версия программного продукта должна работать для всех этих систем.

Для уменьшения затрат, связанных с обучением непосредственных пользователей работе с системой и администраторов в требованиях задается необходимость создания справочной системы. Определены требования к инсталляционному пакету, который с одной стороны должен быть стандартным, с другой обеспечивать возможность автоматической настройки параметров почтовых программ и администрирования пользователей системы.

Выполненный этап планирования позволил создать сценарий использования системы, тестирование которого показало необходимость рассмотрения дополнительного требования по работе с чужой почтой

Опыт работы с украинскими пользователями показывает, что система должна поддерживать многоязыковый интерфейс (украинский, русский, английский). Для обеспечения этой услуги все ресурсы системы реализованы в виде DLL, подключение требуемой DLL на этапе инсталляции фактически определяет язык общения. В дальнейших версиях предполагается возможность смены языка «на лету».

На этапе реализации для максимального учета требования много платформенности не использовались специальные компоненты конкретных быстрых сред разработки. Не использовались также специальные технологии Microsoft типа Active X. Применялась технология сокетов, которая поддерживается для всех современных ОС, используемых для работы с Интернет. Это позволило не только упростить проблему перехода на другие операционные системы, но и уменьшило размер кода, загруженного в памяти. Это важно, так как программа должна быть загружена во все время использования защищенной почты.

Использование технологии сокетов делает разработанное программное обеспечение универсальным с точки зрения возможности использования как при построении систем защиты в глобальной сети, так и в локальных сетях. Отличие состоит лишь в том, что серверный сокет должен «слушать» другой порт (порты). Действительно, для непосредственной работы с Internet Explorer достаточно перехватывать информацию с 80 порта, аналогично работают системы с портами локальной сети.

Система защиты выполняет следующие функции при отсылке письма:

- подпись всех компонентов письма, в том числе предмета, тела письма и прикрепленных файлов;
- шифрование всех компонентов письма, в том числе предмета, тела письма и прикрепленных файлов (необязательный режим);
- запись фамилии подписавшего почту в тело письма в зашифрованном виде;
- экспортирование ключа шифрования и запись его в теле письма в защищенном виде;
- отметка письма как зашифрованного;
- регистрацию выполняемых криптографических операций.

Система защиты выполняет следующие функции при приеме письма:

- импортирование ключа шифрования;
- расшифровку всех компонентов письма, перечисленных выше;
- проверку подписи с учетом всех компонентов письма;
- вывода информации о полученном письме с фамилией подписавшего;
- архивирование полученной почты с цифровой подписью.
- регистрацию выполняемых криптографических операций.

Особое внимание уделено проблеме управления ключевыми данными. Фактически используется 3 модели управления ключевыми данными. Первая модель применяется, если пользователи доверяют центру управления и сертификации ключей. В этом случае в системе предполагается наличие пользователей центра, всем пользователям центр генерирует ключи и передает вместе с личным ключом базу открытых ключей всех пользователей. Это одноуровневый центр, который обеспечивает взаимодействие каждого пользователя с каждым. При смене ключевых данных одного из пользователей выполняется распространение его ключей с использованием защищенной почты. На клиентском месте выполняется импортирование этих ключей с помощью дополнительной утилиты.

Вторая модель предполагает наличие двух уровневого центра. Эта модель используется, если пользователи не доверяют центру генерацию своих ключей. Центр выполняет сертификацию и распространение этих ключей для обеспечения взаимодействия каждого с каждым.

Последняя модель учитывает многоуровневую систему, в которой используются центры разных уровней, которые позволяют при минимальном количестве ключей обеспечить гибкую систему передачи их в соответствии с заданной конфигурацией системы. Ключи каждый пользователь генерирует сам. Оперативно можно изменять конфигурацию системы.

Для дистанционного образования используется упрощенная первая модель, которая должна обеспечить связь между преподавателями и слушателями, но не слушателями между собой. В этом случае преподаватели являются пользователями центра (кафедры, отвечающей за подготовку слушателей). Слушатели являются клиентами системы, каждый слушатель имеет одно рабочее место. Таким образом, преподаватель имеет базу ключей всех своих слушателей, слушатель имеет базу открытых ключей всех своих преподавателей.

Как и всякая система защиты, данная система регистрирует все события, которые происходят, а именно использование ключевых данных, выполнение криптографических операций. Так как использование системы может быть достаточно интенсивным, протокол создается в начале каждого дня, предыдущие протоколы архивируются с датой их создания и цифровой подписью. В настоящей версии полученные сообщения после расшифровки могут быть записаны в файл, определенный пользователем вместе с цифровой подписью. Так как для функционирования системы требуется программное обеспечение для защищенной почты и стандартные почтовые программы, а также личный ключ, почта может быть отправлена в защищенном виде с любого компьютера, достаточно иметь необходимое программное обеспечение и личный ключ.

Разработан тестовый вариант системы, который позволяет для одного пользователя с использованием фиксированного ключа выполнять все операции защищенной почты. Тестовый ключ «зашит» в программе, поэтому не требуется создание личного ключевого носителя.

Исследованы вопросы криптографической стойкости системы. В данной системе применяется режим использования ключей максимальной длины для цифровой подписи (1024 битный вариант). Для передачи ключевых данных используется состоятельный протокол.

Особое внимание уделено вопросам производительности системы. Если для работы с E-mail используется модемное соединение, время, необходимое для криптографических преобразований не превосходит времени для передачи сообщения, поэтому эта проблема остро не стоит. В случае применения выделенных линий использование защиты может существенно повлиять на производительность всей системы. С целью уменьшения потерь времени нами проанализированы методы управления памятью с целью выбора наиболее эффективного метода, который предоставляется операционной системой.

Таким образом, в данной работе предложена технология адаптации MSF модели для разработки систем защиты и получена действующая система, удовлетворяющая современным требованиям к подобным системам и использующая национальные криптографические алгоритмы.

Режимы использования защищенной почты для дистанционного образования.

Слушателю выдается компакт диск, на котором записано все необходимое информационное обеспечение и инсталляционные пакеты для установки защищенной почты и криптографического рабочего места, а также ключевая дискета с паролем входа. Для обеспечения защищенной передачи данных слушателю необходим компьютер с установленной программой для электронной почты (почтовый клиент), который поддерживает протоколы SMTP, POP3[1], подключенный к Интернет. Примерами таких почтовых клиентов являются Outlook Express, The Bat!, MS Outlook. Используя инсталляционный пакет для установки криптографического места, пароль установки и ключевую дискету, пользователь устанавливает на компьютере криптографическое рабочее

[1] Данные протоколы поддерживаются всеми почтовыми клиентами за исключением специализированных почтовых систем

место. На одном компьютере может быть установлено любое число криптографических рабочих мест, что упрощает групповое использование компьютеров, например, в Интернет кафе. Используя инсталляционный пакет для защищенной почты, пользователь устанавливает защищенную почту. Если на одном компьютере работает несколько человек, защищенную почту необходимо установить только один. При инсталляции защищенной почты автоматически формируется учетная запись для работы в защищенном режиме. Для этого инсталлятор запускает программу формирования учетной записи для почтового клиента, выбранного при установке. Если программное обеспечение для защищенной почты уже установлено, новый пользователь должен зарегистрироваться после установки своего криптографического рабочего места. Для этого запускается программа из инсталляционного пакета защищенной почты. После добавления пользователя в адресную книгу стандартными средствами почтовой программы, настройка почты завершается.

Для работы в защищенном режиме достаточно запустить программу защищенной почты и зарегистрироваться (ввести свое криптографическое имя и пароль), а также вставить свой личный ключевой носитель.

Установка защищенной почты не исключает возможности работы с открытой почтой. Для пересылки открытой почты достаточно иметь соответствующую учетную запись. При приеме почты программа автоматически определяет, пришла защищенная или обычная почта. В последнем случае пользователь уведомляется о приеме открытой почты. Если приходит защищенная почта, для письма указывается, кто ее подписал. В случае наличия нескольких пользователей и приеме чужой почты, она сохраняется. В папку полученных сообщений кладется сообщение о приеме письма для пользователя <имя>. После регистрации указанного пользователя его письмо, полученное ранее, «принимается» и регистрируется как все новые письма.

Несмотря на простоту использования защищенной почты, разработчики предлагают достаточно полную систему помощи. Для избежания недоразумений, связанных с неправильным использованием защищенного режима, слушатели при получении инсталляционных пакетов, обучаются установке и работе с защищенной почтой. Как показывает практика использования, слушатели, которые знают основы компьютерной техники и умеют работать с почтовыми программами, на обучение тратят не более 0.5 часа. Для неподготовленных слушателей требуется несколько часов для изучения простейших приемов работы с мышкой, запуска программы и т.д. Администратор почтовой программы в центре должен обучаться в течение нескольких часов.

Таким образом, использование защищенной почты обеспечивает надежную связь между слушателями и преподавателями. Система поддерживает хранение архива всех писем в подписанном виде, что может использоваться при необходимости разрешения конфликтных ситуаций. Срок действия ключей выбирается с учетом срока обучения, поэтому задача смены ключей из-за истечения срока действия ключей не актуальна. Актуальной является проблема смены рабочих ключей из-за выхода из строя ключевого носителя (дискеты). Данную проблему можно разрешить, если личный ключ писать на

информационный CD-ROM или использовать более надежные ключевые носители для хранения личных ключей. Каждое из этих решений имеет недостатки. Использование информационного CD ROM делает необходимым создание уникального CD-ROM для каждого слушателя, использование более надежных ключевых носителей, например Touch memory, Smart Card удорожает систему, так как требует дополнительных затрат на носители и считыватели для них. Поэтому в настоящее время выбрана дискета, программное обеспечение позволяет сделать ее копию, что рекомендуется слушателям выполнять перед первым использованием ключевого носителя.

После истечения срока нельзя переслать защищенное сообщение, но подпись может быть проверена с помощью старых ключей, поэтому можно установить достоверность всей переписки. Таким образом, исключается несанкционированное использование данной системы вне системы дистанционного образования.

В данном докладе рассмотрены вопросы использования защищенной почты для дистанционного образования. Предлагаемый программный продукт можно использовать и для других приложений, когда требуется надежный обмен подписанной и зашифрованной почтой. В рассматриваемой системе используется сертифицированная библиотека Стандартов Украины, которая включает в себя следующие алгоритмы: ГОСТ 34.310-95, ГОСТ 34.311-95, ГОСТ 28.147-89. Система является открытой, т.е. криптографические алгоритмы могут быть заменены с учетом принимаемых Стандартов. Так, в настоящее время на Украине ведутся интенсивные работы в области рассмотрения новых стандартов для симметричной и несимметричной криптографии. При разработке центра управления и сертификации ключей для форматов ключей выбран стандарт X.509, что делает данную ключевую систему совместимой с международными системами защиты информации.

— ◙ —

Информационная система массового доступа по радиотрансляционной сети

Семенец В.В., Татарчук С.И., Курицын В.Н., Осипов Ю.Б.,
Подпружников П.М., Радченко В.И.
Харьковский национальный университет радиоэлектроиики
Харьков, Украина

Abstract

The brief historical help is reduced. The structure of threelinks network of wire broadcasting is reviewed and the brief characteristic of the radiotransmitting network is reduced. The problem of wire broadcasting network possibility as physical area for data transfer is elucidated. The