XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.179-180

УДК 004.773.3.056

Д.О.Сергеев (5 курс, каф. РВиКС), Е.А.Крук, д.т.н., проф.

РАЗРАБОТКА ЗАЩИЩЕННОГО СЕГМЕНТА ЭЛЕКТРОННОЙ ПОЧТОВОЙ СИСТЕМЫ (ЗС ЭПС)

Ведение служебной переписки между корреспондентами ЭПС МПС России предполагает пересылку не только общедоступной, но и конфиденциальной информации, информации для служебного пользования и т.п. В связи с этим возникает необходимость организовать защищенный обмен между субъектами информационных взаимоотношений, осуществлять их однозначную аутентификацию и централизованное управление аутентификационной информацией с использованием сертифицированных средств криптозащиты. Для ведения закрытой переписки корреспонденты должны обладать возможностью выполнять стандартные операции такие как шифрование сообщения, подпись сообщения, дешифровка сообщения, проверка подписи сообщения, работа с сертификатами безопасности.

В связи с этим возникает необходимость разработки такого средства как ЗС ЭПС МПС РФ. Основным предназначением ЗС является организация взаимодействия между рядом абонентов ЭПС МПС РФ в режиме защиты передаваемой и хранимой на рабочих местах информации от несанкционированного доступа. Защищенный сегмент включает в себя ограниченный набор рабочих мест ЭПС МПС России. Перемещение рабочего места из ЭПС МПС России в защищенный сегмент должно производиться путем инсталляции на рабочем месте специального программного обеспечения, позволяющего осуществлять функции защиты при работе с сообщениями. Обмен информацией между рабочими местами, входящими в защищенный сегмент, происходит с использованием тех же каналов связи, что и при работе других рабочих мест, входящих в ЭПС МПС России. Таким образом, защищенный сегмент функционирует как логическая подсистема ЭПС МПС России.

ЗС состоит из следующих основных структурных единиц:

- Центр Сертификации. Функции:
  - управление пользователями и администраторами;
  - изготовление и отзыв сертификатов;
  - управление публикацией сертификатов.
- Архив секретных ключей. Функции:
  - хранение секретных ключей пользователей;
  - сохранение и выдача секретных ключей.
- WEB-интерфейс пользователя. Функции:
  - регистрация пользователя в Центре Регистрации;
  - создание запросов на выпуск, отзыв и высылку сертификатов;
  - установка выпущенных сертификатов.
- Центр Регистрации. Функции:
  - управление запросами пользователей - принятие решений по регистрации, выпуску, отзыву, высылке сертификатов;
  - регистрация пользователей при их личном обращении в Центр Регистрации;
  - выпуск и отзыв сертификатов для пользователей при их личном обращении в Центр Регистрации.

Для реализации и использования решений, основанных на инфраструктуре открытых ключей, используется криптопровайдер КриптоПро CSP, имеющий сертификат ФАПСИ.

Одной из основных операций, выполняемых пользователями, является электронно-цифровая подпись документов (ЭЦП). Алгоритм формирования и проверки ЭЦП реализован в криптопровайдере в соответствии с требованиями ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма".

В работе рассматривается общая архитектура ЗС ЭПС. В рамках работы наибольшее внимание уделяется применению ЭЦП. Рассмотрены основные схемы ЭЦП, варианты их классификации, способы атаки на ЭЦП.

ЛИТЕРАТУРА:

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone “Handbook of Applied Cryptography”, CRC Press – 1996, 816 p.
2. Введение в криптографию / под общей ред. В.В. Ященко. – СПб.:Питер, 2001. 288 с.
3. КриптоПро CSP, назначение и использование - http://www.cryptopro.ru.
4. Шнайер Б. «Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си», Триумф – 2002. 816 с.