СИСТЕМА ШИРОКОВЕЩАТЕЛЬНОГО ШИФРОВАНИЯ ДЛЯ ЗАЩИТЫ ДАННЫХ В СЕТИ ИНТЕРНЕТ

Койпиш М. Л., Семенов В. И., Соловей О. В.

НИИ прикладных проблем математики и информатики Белгосуниверситета, Минск, Беларусь, e-mail: apmi@bsu.by

Данные могут передаваться путем широковещательной рассылки от одного источника сразу всем пользователям информационной системы. При этом защита предаваемых данных предусматривает шифрование, контроль целостности, а также контроль доступа: любой пользователь может получить зашифрованные данные, но только определенные пользователи, не включенные в список запрещенных, могут выполнить их расшифрование и контроль целостности. Если общее число пользователей велико и состав запрещенных пользователей меняется динамично, то для организации защиты можно использовать протоколы широковещательного шифрования (ПШШ) [1]. В докладе рассматривается система широковещательного шифрования (СШШ), основанная на использовании ПШШ SD [1].

СШШ строится по принципу «клиент – сервер», где клиентами являются пользователи системы, размещающие и получающие целевую информацию (ЦИ) в защищенном виде, а сервер выполняет функции по генерации и распределению ключей ПШШ, контролю доступа к ЦИ, хранению ЦИ в защищенном виде и др.

В СД сервер логически разделяется на сервер контроля доступа (СКД), сервер хранения информации (СХИ) и сервер распределения ключей (СРК). Пользователи взаимодействуют со всеми серверами.

СКД при получении от пользователя запроса на размещение ЦИ анализирует установленные в запросе права доступа к ЦИ и формирует на их основе определенный заголовок, используемый в ПШШ при установке защиты на ЦИ. После защиты ЦИ пользователем СКД размещает защищенную ЦИ на СХИ.

СХИ хранит защищенную ЦИ, включающую заголовок и зашифрованную ЦИ с имитовставкой. По заголовку любой пользователь СД может определить, является ли он разрешенным для данной ЦИ или нет. Разрешенные пользователи, применяя ПШШ, могут снять защиту с ЦИ с использованием заголовка и своих ключей.

СРК регистрирует пользователей, генерирует и распределяет ключи пользователей и СКД, используемые в ПШШ при установке и снятии защиты.

Для аутентификации клиентов и серверов, а также для безопасного распределения ключей пользователям используются алгоритмы электронной цифровой подписи и транспорта ключей, соответствующие СТБ 34.101.45.

Клиентское ПО системы предлагается строить следующим образом. Веб-приложение на основе javascript получает ЦИ от СХИ и передает ее локальной клиентской программе (КП) по протоколу websockets. КП снимает защиту с ЦИ и возвращает ее веб-приложению для дальнейшей обработки. Перспективным представляется обработка расшифрованного видео-контента, который помещается внутрь тега video на веб-странице и воспроизводится средствами браузера с поддержкой html5.

Литература