**Лекция №12. Электронная цифровая подпись**

**Цель лекции:** иметь представление о методе аутентификации отправителя или автора подписи, подтверждающий, что содержание документа не было изменено.

**Содержание лекции:** односторонняя хеш-функция, цифровая подпись.

Для того, чтобы объяснить механизм цифровой подписи, необходимо ввести понятие односторонней хеш-функции. Односторонняя хеш-функция - это функция, которая преобразует исходное послание любой длины в строку символов ограниченной длины - так называемый дайджест послания. При использовании 16-байтной хеш-функции вы на выходе получите запись длиной 16 байт. Даже если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, все равно остается возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют контрольной суммой, или дайджестом сообщения. Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений. Алгоритмы расчета контрольных сумм разработаны так, чтобы они были по возможности уникальны для каждого сообщения. Таким образом устраняется возможность подмены одного сообщения другим с сохранением того же самого значения контрольной суммы. Однако, при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей ее решения является включение контрольной суммы в так называемую электронную подпись. При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определенные права отправителем. Электронные цифровые подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число - порядковый номер. более подробно о электронной цифровой подписи (ЭЦП) читайте в разделе курса ОСВМ Аутентификация информации. С 2012 года в Казахстане функционирует свой Национальный удостоверяющий центр, в котором граждане и организации Казахстана могут получить свои закрытые ключи и программные пакеты для формирования своей цифровой подписи для ведения электронных юридических операций с ее использованием. Необходимо, 47 однако, заметить, что данная система еще очень сырая и позволяет злоумышленникам легко воспользоваться чужой электронной подписью для совершения подложных сделок. Это происходит по следующим причинам: выдача файлов электронных подписей совершается «вручную», то есть оператор, выдающий подпись всегда может иметь ее копию на своем USBносителе, пароль выдается на всех один (!!!) - 123456. При попытке смены пароля файл электронной подписи записанный на стираемом носителе, фатально повреждается, и, если владелец подписи не сделал предварительно копию, то он лишается возможности подписывать документы до получения новой подписи из НУЦ, ЦОН или у программистов районного налогового комитета. На сегодня уже известно множество фиктивных сделок с недвижимостью и иным имуществом, а также незаконным получением документов с помощью чужой электронной подписи. Поэтому, единственно разумным действием, предохраняющим человека от лишения его собственности. Хеширование – это одностороннее, т. е. необратимое, в отличие от шифрования, преобразование. По дайджесту послания нельзя восстановить исходное сообщение, но можно его однозначно идентифицировать. Рассмотрим конкретный пример. Пусть А, применив хеш-функцию, получил дайджест в виде некоего кода (код1). Затем, используя свой личный ключ, А зашифровывает дайджест, который и становится аналогом подписи данного документа. Далее А отправляет открытый текст послания и цифровую подпись В. Абонент В расшифровывает подпись публичным ключом, который он получил от А и убеждается, что письмо действительно от А Таким образом, аутентификация состоялась. Затем необходимо удостовериться, что послание не было изменено в процессе доставки. В результате расшифровки В получает дайджест послания - код1. Затем В, используя ту же хеш-функцию, что и А, хеширует текст послания и получает дайджест в виде некоторого кода2. Если код1 и код2 совпадают, то В делает вывод о том, что текст послания не был изменен на этапе доставки. Таким образом, цифровая подпись или электронная подпись – это метод аутентификации отправителя или автора подписи, подтверждающий, что содержание документа не было изменено. Цифровая подпись может быть поставлена как в зашифрованном, так и в открытом послании.