Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №5**

**«Криптографическая защита информации»**

Выполнил:

Студент 2 курса 1 группы ФИТ

Палазник Арсений Викторович

Цель: изучить и закрепить умение реализации ЭЦП на примере RSA.

Контрольные вопросы:

1. Дайте определение понятию "электронная цифровая подпись".

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

1. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.

При создании цифровой подписи по классической схеме отправитель:

* применяет к исходному сообщению T хеш-функцию h(T) и получает хеш-образ r сообщения;
* вычисляет цифровую подпись s по хеш-образу r с использованием своего закрытого ключа;
* посылает сообщение T вместе с цифровой подписью s получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

* применяет к полученному сообщению T хеш-функцию h(T) и получает хеш-образ r сообщения;
* расшифровывает хеш-образ r’ из цифровой подписи s с использованием открытого ключа отправителя;
* проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

1. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?

Порядок использования ключей обратный тому, который используется при передаче секретных сообщений. В начале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

1. Опишите схему протокола ЭЦП на основе алгоритма RSA.



1. Перечислите специальные схемы ЭЦП.

Кроме классической схемы ЭЦП различают еще несколько специальных:

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
* схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано.