Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №7*

ТЕМА ЗАНЯТИЯ: ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

Цель: изучить и закрепить умение реализации электронноцифровой подписи на примере RSA.

**Краткие теоретические сведения**

Электронная цифровая подпись (ЭЦП) – это криптографический механизм, который обеспечивает подлинность отправителя и целостность передаваемых данных. Она играет важную роль в современных системах электронного документооборота, банковских операциях, государственных услугах и других сферах, требующих защиты информации. ЭЦП является аналогом традиционной подписи, но используется для подтверждения авторства цифровых документов.

Основными свойствами ЭЦП являются аутентификация, целостность данных и невозможность отказа от авторства. Аутентификация гарантирует, что документ подписан именно тем лицом, которому принадлежит подпись. Целостность данных означает, что информация в документе не была изменена после подписания. Невозможность отказа от авторства предотвращает ситуации, когда отправитель может отрицать факт подписания документа.

Существует несколько алгоритмов формирования и проверки ЭЦП. К наиболее распространенным относятся RSA, DSA, Эль-Гамаля и Шнорра. Алгоритм RSA основан на сложности разложения больших чисел на множители, DSA использует модульную арифметику, а Эль-Гамаля и Шнорра базируются на сложности вычисления дискретного логарифма.

Благодаря своей надежности и юридической значимости, ЭЦП широко используется в различных сферах. Она применяется в системах электронного документооборота, онлайн-банкинге, при подписании цифровых контрактов, в государственных услугах и защите конфиденциальной информации.

**1. Объясните последовательность выполнения процедур генерации и проверки ЭЦП.**

Электронно-цифровая подпись (ЭЦП) создается и проверяется в несколько этапов:

Генерация ЭЦП:

1. Вычисление хэш-образа: исходное сообщение подвергается хэшированию с использованием криптографической хэш-функции, например, SHA-256.
2. Шифрование хэш-образа: хэш-образ подписывается с использованием закрытого ключа отправителя с помощью алгоритма цифровой подписи, такого как RSA или Эль-Гамаля. Это создает электронную цифровую подпись.
3. Отправитель посылает сообщение вместе с цифровой подписью получателю.

Проверка ЭЦП: Получатель:

1. Отделяет электронную цифровую подпись от исходного сообщения.
2. Вычисляет хэш-образ из цифровой подписи с использованием открытого ключа отправителя.
3. Вычисление хеш-образа исходного сообщения.
4. Полученный хэш-образ сравнивается с вычисленным хэш-образом исходного сообщения. Если они совпадают, подпись считается верной, а сообщение - неизменным и аутентичным.

**2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.**

**Отправитель:**

1. Генерирует пару ключей - закрытый и открытый ключи. Закрытый ключ остается у отправителя, а открытый ключ распространяется для использования при проверке ЭЦП.
2. Берет исходное сообщение, которое требуется подписать, и применяет к нему хэш-функцию для получения хэш-образа.
3. Использует свой закрытый ключ для шифрования хэш-образа. Это создает электронную цифровую подпись.
4. Посылает сообщение вместе с цифровой подписью получателю.

**Получатель:**

1. Получает исходное сообщение с ЭЦП.
2. Отделяет электронную цифровую подпись от исходного сообщения.
3. Использует открытый ключ отправителя для расшифровки электронной цифровой подписи и получает хэш-образ, который был использован отправителем.
4. Применяет ту же хэш-функцию к полученному исходному сообщению и вычисляет хэш-образ.
5. Полученный хэш-образ сравнивается с расшифрованным хэш-образом, полученным из электронной цифровой подписи. Если они совпадают, подпись считается верной, а сообщение - неизменным и аутентичным.

**3. Опишите схему протокола ЭЦП на основе алгоритма RSA.**

**1. Генерация ключей (на стороне отправителя)**

1. Выбираются два больших простых числа p и q;
2. Вычисляется их модуль n = p\*q;
3. Далее вычисляется функция Эйлера φ = (p - 1)(q - 1);
4. Выбирается открытая экспонента e, которая является взаимно простой с φ(n);
5. Вычисляется секретная экспонента ;
6. В итоге получаются ключи:

**Открытый ключ**: (e,n) – используется для проверки подписи.

**Закрытый ключ**: (d,n) – используется для подписания данных.

**Список использованных источников**

1. Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ Лабораторный практикум