**Лекция 7: Виды средств контроля целостности данных, цифровые подписи и сертификаты.Технологии контроля целостности данных.**

Роль цифровых подписей и сертификатов в обеспечении безопасности.

Применение цифровых подписей для проверки подлинности и целостности данных.

**Средства контроля целостности данных** - это важный аспект обеспечения безопасности информации. Они предназначены для обнаружения любых изменений или повреждений данных в процессе их передачи или хранения. Вот некоторые из основных технологий контроля целостности данных:

1. **Хэширование данных:** Хэширование - это процесс преобразования данных произвольной длины в фиксированную строку фиксированной длины (хэш-значение). Любое изменение исходных данных, даже самого маленького бита, приведет к значительному изменению хэш-значения. Это позволяет обнаруживать даже небольшие изменения в данных.
2. **Цифровые подписи:** Цифровая подпись - это способ аутентификации отправителя и обеспечения целостности сообщения. Отправитель создает хэш-значение сообщения и подписывает его своим закрытым ключом. Получатель может проверить подлинность и целостность сообщения, используя открытый ключ отправителя.
3. **Сертификаты:** Сертификаты используются для связывания открытых ключей с конкретными субъектами (пользователями, устройствами и др.). Сертификаты выдаваются доверенными удостоверяющими центрами (Центрами сертификации), и они подтверждают, что открытый ключ принадлежит указанному субъекту.
4. **Контрольные суммы (Checksums):** Контрольные суммы - это числа или значения, вычисляемые на основе данных, которые можно использовать для проверки целостности данных. При получении данных получатель также вычисляет контрольную сумму и сравнивает ее с переданной контрольной суммой. Если они не совпадают, это указывает на повреждение данных.

**Цифровые подписи** и **сертификаты** играют ключевую роль в обеспечении безопасности, предоставляя следующие возможности:

* **Подлинность:** Цифровая подпись подтверждает, что сообщение или данные были созданы конкретным отправителем или субъектом и не были изменены в процессе передачи.
* **Целостность:** Цифровая подпись также гарантирует, что данные остались неизменными с момента подписания.
* **Аутентификация:** Сертификаты позволяют подтверждать личность субъекта, а также подтверждают, что его открытый ключ действителен и принадлежит ему.
* **Доверие:** Использование доверенных центров сертификации позволяет установить доверие к открытым ключам и сертификатам, таким образом, снижая риск атак, связанных с подделкой.

**Применение цифровых подписей**:

1. **Электронные транзакции:** Цифровые подписи используются в онлайн-банкинге, электронной коммерции и других сферах для подтверждения подлинности и целостности финансовых транзакций.
2. **Электронные документы:** Цифровые подписи могут быть прикреплены к электронным документам (например, PDF) для подтверждения авторства и невозможности изменения документа после подписания.
3. **Электронная почта:** Цифровые подписи могут использоваться для шифрования и аутентификации электронной почты, обеспечивая конфиденциальность и безопасность коммуникаций.
4. **Веб-сайты:** SSL/TLS сертификаты используются для защищенной передачи данных между пользователем и веб-сайтом, обеспечивая безопасность при вводе личной информации и паролей.

Цифровые подписи и сертификаты являются важными инструментами в сфере информационной безопасности, обеспечивая доверие, целостность и аутентификацию данных и коммуникаций.

Пример Python-кода для создания цифровой подписи и ее проверки с использованием библиотеки **cryptography**. В этом примере мы также используем хэширование данных для обеспечения целостности.

















**verify** используется для проверки подписи. Если подпись верна, выводится "Подпись верна. Данные целы и подлинны."