



Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
профессионального образования «Московский государственный технический университет
имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

Основы обеспечения информационной безопасности

Криптографические методы защиты информации

Кафедра «Защита информации»



Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.



Шифрование - процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.



«Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

Основы обеспечения информационной безопасности

СКЗИ (средство криптографической защиты информации) — программа (служба), которая обеспечивает шифрование и цифровую подпись на рабочей станции. Применение эффективных криптографических алгоритмов позволяет:

- ✓ шифровать различные документы (накладные, отчеты и так далее);
- ✓ расшифровывать ответы, полученные от контрагентов, а также протоколы от различных организаций – ИФНС, ПФР, Росстат;
- ✓ проверять секретные ключи пользователя при отправке электронных документов по каналам связи.





Симметричное шифрование

Симметричное шифрование — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в тайне обеими сторонами, осуществляться меры по защите доступа к каналу, на всем пути следования криптограммы. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.





Асимметричное шифрование

Симметричное шифрование — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в тайне обеими сторонами, осуществляться меры по защите доступа к каналу, на всем пути следования криптограммы. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.





«Московский государственный технический университет имени Н.Э. Баумана» (МГТУ им. Н.Э. Баумана)

Основы обеспечения информационной безопасности

Электронная подпись (ЭП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).





«Московский государственный технический университет имени Н.Э. Баумана» (МГТУ им. Н.Э. Баумана)

Основы обеспечения информационной безопасности

Сертификат электронной подписи – документ, который подтверждает принадлежность открытого ключа (ключа проверки) ЭП владельцу сертификата.
Владелец сертификата ЭП – физическое лицо, на чье имя выдан сертификат ЭП в удостоверяющем центре.

Закрытый ключ электронной подписи (ключ ЭП) позволяет генерировать электронную подпись и подписывать электронный документ. Владелец сертификат обязан в тайне хранить свой закрытый ключ.

Открытый ключ электронной подписи (ключ проверки ЭП) однозначно связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП.

Подписывание



Проверка

