МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

И.А. Петриченко, Е.А. Лещенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Распределенные информационные системы (РИС) характеризуются передачей данных между территориально разнесенными компонентами, что повышает риск несанкционированного доступа и утечки конфиденциальной информации. В связи с этим обеспечение информационной безопасности в РИС является ключевой задачей.

Существует 3 основных средства криптографической защиты информации: программные, аппаратные и программно-аппаратные. Их цель состоит в том, чтобы:

– уберечь информацию во время ее изменения, использования и отправки;

– обеспечить целостность и подлинность данных при хранении, обработке и распространении;

– создавать информацию, которая будет применяться для аутентификации и идентификации субъектов, людей и устройств;

– выработать данные, используемые для сохранности аутентифицирующих средств при их хранении, создании, изменении и передаче.

Есть четыре основных метода криптографической защиты информации:

– симметричное шифрование: Использование общего ключа для шифрования и расшифрования данных. Примеры: AES, DES, Blowfish;

– асимметричное шифрование: Использование открытого и закрытого ключей. Примеры: RSA, Эллиптические кривые;

– хэширование: Применение криптографических хэш-функций для обеспечения целостности данных. Примеры: SHA-2, MD5;

– электронная цифровая подпись: Использование закрытого ключа для создания подписи, проверка с помощью открытого ключа. Примеры: DSA, ГОСТ Р 34.10.

Применение криптографических методов и средств является важным элементом обеспечения информационной безопасности в распределенных информационных системах. Их использование позволяет защитить конфиденциальность, целостность и доступность данных, циркулирующих в РИС.

Список литературы

1. Криптографическая защита информации: цели, методы, технологии [Электронный ресурс]. – Режим доступа: https://gb.ru/blog/kriptograficheskaya-zaschita-informatsii/. – Дата доступа: 07.05.2024.