КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ В POS-ТЕРМИНАЛАХ

Э.Д. Альбино Родригес, М.Н. Гиль, В.В. Лобунов

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

В наше время, когда электронные платежи становятся все более распространенными и незаменимыми для современного бизнеса, безопасность и надежность транзакций играют ключевую роль. Криптографические модули в PoS-терминалах становятся фундаментом для обеспечения этой безопасности, обеспечивая защиту конфиденциальности данных и целостности транзакций.

Криптографический модуль представляет собой набор алгоритмов и протоколов, используемых для защиты конфиденциальных данных при передаче информации между терминалом и платежной системой. Принцип работы криптографического модуля основан на использовании сильных криптографических алгоритмов для шифрования данных, таких как алгоритмы шифрования с открытым и закрытым ключом. При совершении платежа данные, такие как номер карты, сумма транзакции и другие важные сведения, защищаются путем шифрования перед их отправкой на сервер платежной системы. После получения данных сервер дешифрует их с помощью соответствующего ключа для обработки транзакции.

Если криптографический модуль становится подвержен атакам или воздействию злоумышленников, это может иметь серьезные последствия. Нарушение безопасности модуля может привести к утечке конфиденциальной информации о платежах и карты пользователя, что в свою очередь может привести к финансовым потерям и потере доверия со стороны клиентов и партнеров компании. Кроме того, такие атаки могут нанести ущерб репутации компании и вызвать юридические последствия, вплоть до штрафов и судебных исков.

В работе рассмотрены механизмы шифрования Triple DES, AES. Также продемонстрированы их работа в реальном времени на платежном терминале PAX A930RTX, уровни защиты от физического / программного воздействия злоумышленника.

Платежные терминалы используются и будут использоваться, так как они существенно упрощают взаимодействие клиента и продавца, ускоряют бизнес-процессы. Однако их функционирование требует мониторинга, соблюдения стандартов безопасности, поиска уязвимостей и их последующего устранения.

Список литературы

1. Стандарт безопасности данных, принятый в индустрии платежных карт PCI DSS [Электронный ресурс]. – Режим доступа: https://listings.pcisecuritystandards.org/ ptsdocs/4-90260%20A930RTX_Securi- ty_Policy-1706898394.63736.pdf. – Дата доступа: 07.05.2024.

2. Механизмы обеспечения безопасности платежа [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles /281438/. – Дата доступа: 07.05.2024.