ОПИСАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ДАННЫХ ШЛЮЗА ПРИЕМА-ПЕРЕДАЧИ ДАННЫХ

Передача данных между Шлюзом приема-передачи данных (ППД) и кассовыми аппаратами осуществляется посредством протокола HTTPS. HTTPS (Hypertext Transfer Protocol Secure) — расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL, тем самым обеспечивается защита этих данных. В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 443.

HTTPS обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от снифферских атак и атак типа man-in-the-middle при условии, что будут использоваться шифрующие средства и сертификат сервера проверен и ему доверяют.

В свою очередь протокол SSL который отвечает за конфиденциальность данных в протоколе HTTPS, собственно обеспечивает установление безопасного соединения между клиентом и сервером (в конкретном случае между кассовым аппаратом и Шлюзом ППД). Протокол SSL состоит из двух подпротоколов: протокол SSL записи и рукопожатия. Протокол SSL записи определяет формат, используемый для передачи данных. Протокол SSL включает рукопожатие с использованием протокола SSL записи для обмена сериями сообщений между сервером и клиентом (клиентом выступает кассовый аппарат) во время установления первого соединения. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат.

SSL предоставляет канал, имеющий 3 основных свойства:

- Аутентификация. Сервер всегда аутентифицируется, в то время как клиент аутентифицируется в зависимости от алгоритма.
- Целостность. Обмен сообщениями включает в себя проверку целостности.
- Конфиденциальность канала. Шифрование используется после установления соединения и используется для всех последующих сообщений.

Для обеспечения работы протокола SSL, а следовательно и HTTPS, встроенные модемы кассовых аппаратов модели MINI-T400ME и сервер Шлюза ППД оснащены проверенными SSL-сертификатами. Следовательно, руководствуясь спецификациями протокола SSL, перед началом передачи данных, кассовые аппараты и Шлюз обмениваются своими сертификатами и происходит процедура рукопожатия, следствием которой является установка безопасного соединения.