Hackers installed the Raspberry Pi mini-computer with a 4G modem inside the network of one bank to access the system of ATMs and try to steal money. This was reported by security experts from Group-IB.

The device was connected directly to the network of ATMs, which gave attackers full access to the internal systems of the bank. Their main goal is to hack the ATM management server and gain control of the protective module that stores important data and is responsible for encryption.

A group of hackers, known as UnC2891, has been operating since 2017 and specializes in attacks on banking systems. Previously, they used complex harmful software, which could be hidden even from professional experts.

In this case, the attackers applied a new way to mask the harmful code to the usual system process, which complicated its detection. They also hacked the bank’s mail server to maintain a constant connection with Raspberry Pi through the monitoring server.

Fortunately, the attack was discovered and stopped before the hackers managed to implement their plans.