**2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ**

**2.1 Назначение системы**

Устройство защиты АТМ от несанкционированных подключений и атак BlackBox, Dispense Switch Manipulation, ATM Malware/Touchless Jackpotting, выполняющее обработку зашифрованных сигналов, посылаемых агентом банкомата на диспенсер.

**2.2 Цели создания системы**

Целями создания системы является создание аппаратной части и программного обеспечения для защиты системной USB шины от несанкционированных подключений, атак BlackBox, Dispense Switch Manipulation, ATM Malware/Touchless Jackpotting.

**4 ТРЕБОВАНИЯ К СИСТЕМЕ**

**4.2. Требования к функциям, выполняемым системой**

**4.2.1 Задачи системы**

Основная задача системы – обеспечение безопасности банкомата. Система должна автоматически определять и блокировать попытку несанкционированного доступа к оборудованию, выводить информацию на веб-интерфейс оператора в случае попытки несанкционированного доступа.

**4.2.2 Функциональные требования к системе**

Система на уровне аппаратных средств вычислительной техники (Контроллер ATM Keeper для банкоматов NCR*/*Wincor) должна обеспечить обнаружение и блокировку, устранение несанкционированных подключений к системной USB шине. Несанкционированным подключением является любое незашифрованное подключение (незашифрованные команды управления), отличное от постоянного.

Веб-интерфейс, развернутый на ПК, должен обеспечить наличие пользовательского интерфейса для возможности администрирования и операторской работы с системой. Веб-интерфейс должен поддерживать функционирование системы, автоматизированную работу по взаимодействию с аппаратной частью системы, а именно получение данных с контроллера ATM Keeper для банкоматов NCR*/*Wincor.

При появлении подозрительных подключений, команд необходимо вывести сигнал, оповещающий систему о несанкционированном доступе, и устранить эту попытку подключения. Сигнал должен быть обработан в виде оповещения оператора в веб-интерфейсе.