**Требования стандарта PCI DSS, предъявляемые к организациям торговли и сервиса**

**Построение и поддержание защищенной сети:**

1. Должны быть обеспечены разработка и управление конфигурацией межсетевых экранов в целях защиты данных платежных карточек.
2. Не должны использоваться параметры безопасности и системные пароли, установленные производителем по умолчанию.

**Построение и поддержание защищенной сети:**

1. Должна быть обеспечена защита данных платежных карточек при хранении.
2. Должно обеспечиваться шифрование данных платежных карточек, передаваемых по сетям общего пользования.

**Реализация программы управления уязвимости:**

1. Должно использоваться и регулярно обновляться антивирусное программное обеспечение.
2. Должна обеспечиваться безопасность при разработке и поддержке систем и приложений.

**Реализация мер по строгому контролю доступа:**

1. Доступ к данным платежных карточек должен быть ограничен в соответствии со служебной необходимостью.
2. Каждому лицу, имеющему доступ к вычислительным ресурсам, должен быть назначен уникальный идентификатор.
3. Физический доступ к данным платежных карточек должен быть ограничен.

**Регулярный мониторинг и тестирование сетей:**

1. Должен отслеживаться и контролироваться любой доступ к сетевым ресурсам и данным платежных карточек.
2. Должно выполняться регулярное тестирование систем и процессов обеспечения безопасности.

**Поддержание политики информационной безопасности:**

Должна поддерживаться политика информационной безопасности, регламентирующая деятельность сотрудников и контрагентов.