Для организаций, которые подключают услугу электронной коммерции (e-commerce) через банк, существует ряд требований в области информационной и кибербезопасности. Эти требования направлены на обеспечение защиты данных, транзакций и соблюдение стандартов безопасности.

1. Соответствие стандарту PCI DSS

- Хотя непосредственно ответственность за соблюдение стандартов PCI DSS ложится на **мерчантов**, они обязаны принимать меры по защите данных клиентов (например, номера карт). Это включает:
    - Не хранить данные карты. (PAN, CVV, CARDHOLDER NAME, EXP DAY)
    - Защищать передаваемые данные с помощью шифрования (не ниже TLSv 1.2).

2. Использование безопасных протоколов связи

- Мерчанты обязаны внедрить защищенные каналы передачи данных с использованием **HTTPS (не ниже TLSv 1.2)** для защиты транзакций и данных пользователей при обмене информацией с сайтом банка или платёжной системой.

3. Многофакторная аутентификация (MFA)

- Включение **многофакторной аутентификации** для входа в личный кабинет клиента или доступа к процессинговым сервисам банка, чтобы повысить безопасность доступа к аккаунтам, которые используют e-commerce сервисы.

4. Защита от атак

- Установление защитных механизмов для предотвращения таких атак, как **SQL-инъекции**, **межсайтовый скриптинг (XSS)**, **DDoS** и другие уязвимости. Это важно для обеспечения безопасности веб-сайтов и платформ, через которые проходят транзакции.
- Защита от **фишинга** и других мошеннических схем, а также обучение пользователей безопасному поведению в сети.

5. Обновления и патчи безопасности

- Мерчанты должны регулярно обновлять свои системы и программное обеспечение, чтобы минимизировать риски, связанные с уязвимостями, которые могут быть использованы злоумышленниками.

6. Шифрование данных

- Шифрование личных данных и данных платежных карт как при передаче, так и при хранении. Это требование касается как хранения транзакционных данных, так и информации о клиентах.

7. Обучение сотрудников

- Проведение регулярных тренингов по безопасности для сотрудников компании, включая обучение мерам защиты от фишинга, социального инженерства и других угроз безопасности.

8. Контроль доступа

- Установление строгих политик контроля доступа для сотрудников, имеющих доступ к системе обработки платежей или данным клиентов. Например, доступ к информации о

платежах должен быть ограничен только теми сотрудниками, которым это необходимо для выполнения своих обязанностей.

9. Регулярные аудиты и тестирование

- Проводить регулярные **аудиты безопасности** и тесты на проникновение для выявления уязвимостей в системе, а также для обеспечения соответствия стандартам безопасности.

10. Ответственность за безопасность

- Продавцы, подключающие услуги электронной коммерции через банк, должны понимать свою ответственность за обеспечение безопасности транзакций, данных клиентов и соблюдение всех соответствующих стандартов.