КОНСОРЦИУМ ЮМИРА

COS PCI PIBRS

«Стандарт платежной индустрии о запросах при покупке»

НА ОДОБРЕНИИ

О стандарте

Стандарт необходим для стандартизации запросов сайтов для покупок с использованием платежных систем. В частности, это облегчит работу платежных систем и сайтов с совершением таковых запросов.

Глава 1. Минимальные данные

Для безопасности, клиент (пользователь, совершающий операцию на сайте) должен вводить только минимальные данные. Чем меньше данных пользователь вводит на стороннем сайте, тем больше шанс, что платежное средство не будет взломано. Рекомендованный список минимальных данных:

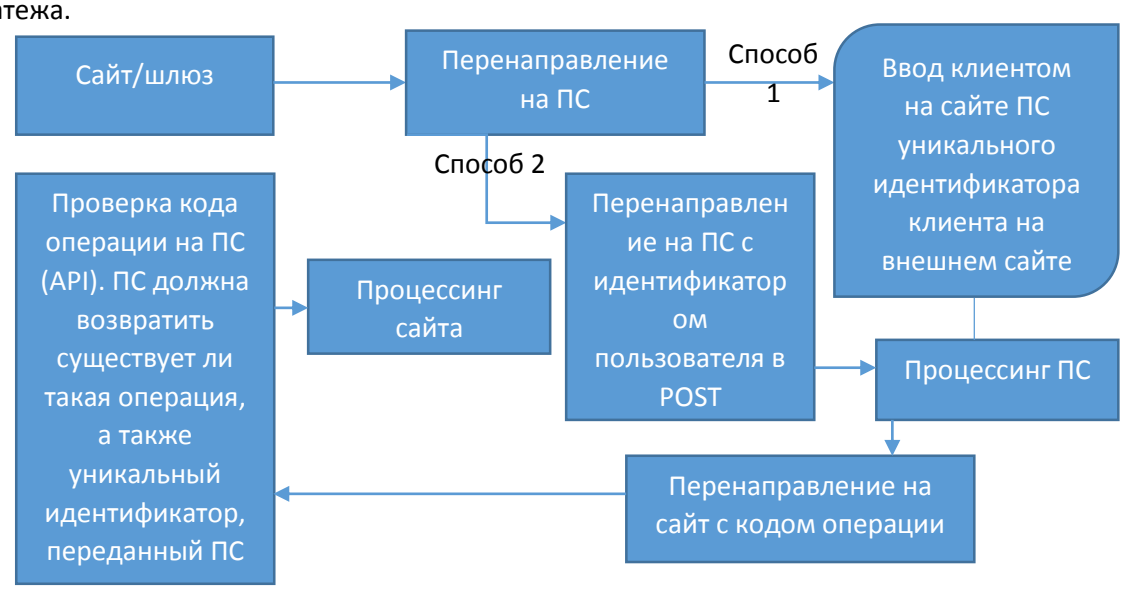
1. Card PAN (Primary Account Number)
2. VALID THRU
3. Cardholder
4. 3-Digit Security Code*
5. 3DS Checking*

3-Digit Security Code может вводиться только на шлюзах, сертифицированных PCI DSS отдельно. Если такового сертификата шлюз не имеет, код должен вводиться на сайте платежной системы. Платежная система может изменять 3-Digit Security Code по усмотрению, например, он может быть буквенным и содержать 4 символа. Так же, обращаем внимание, что сертифицированы могут быть только шлюзы (сервис, который предлагает подключиться к нему другим сайтам для приема платежей), а не отдельный веб-сайт. Это означает, что, если сайт работает без шлюза, такого сертификата он не имеет, и платежная система должна принимать этот код уже на своей стороне.

3DS Checking не является **обязательным** методом, однако, он рекомендован, так как вероятность взлома очень сильно снижается.

Глава 1.2. Для электронных кошельков

Электронные кошельки, конечно, могут использовать точно такую же форму, как и «кардовые» ПС, однако, скорее всего гораздо легче перенаправить пользователя на сайт электронного платежа.



Если платежная система хочет использовать такую же форму, как и кардовую, минимальный набор данных данный документ не устанавливает.

Глава 2. Запросы от сайта к платежной системе

Сайт/шлюз должен отправить минимальные данные на сайт платежной системы через POST. При этом, он должен отправить код операции на своем сайте. Далее, платежная система должна попросить пользователя ввести 3-Digit Security Code, если таковый код не был передан сайтом/шлюзом. Если такой код был передан, то платежная система должна сразу перейти к 3DS Checking, если таковой имеется, или, если таковой проверки не имеется, то сразу перейти к своему процессингу. Далее, платежная система должна отправить на сайт/шлюз в формате POST код операции на сайте/шлюзе, код операции на ПС, Card PAN (сайт должен его хранить до окончания операции), и другие данные для валидации. Далее, сайт/шлюз должен проверить эти данные через API ПС. Далее, если данные в БД сайта и БД платежной системы совпадают, операция может считаться завершенной.–