Разъяснение процедуры безопасной передачи конфиденциальной информации Держателей

1. Общие положения

Настоящее разъяснение определяет порядок безопасной передачи по каналам связи конфиденциальной информации Держателей банковских карт (далее — Данные).

К конфиденциальной информации относятся:

- номер банковской карты
- срок действия карты
- имя Держателя карты
- код безопасности (CVV/CVC)
- иные платёжные реквизиты

---

2. Основные принципы безопасности

Передача Данных осуществляется с соблюдением следующих принципов:

- конфиденциальность — исключение доступа третьих лиц
- целостность — защита от изменения при передаче
- подлинность — подтверждение источника данных

---

3. Безопасные каналы передачи

Передача конфиденциальной информации Держателей осуществляется исключительно с использованием защищённых каналов связи, включая:

- протокол HTTPS (TLS-шифрование)
- защищённые платёжные страницы платёжных провайдеров
- встроенные (hosted) платёжные формы

Использование открытых и незащищённых каналов связи (например, email, мессенджеры, SMS) для передачи полных реквизитов банковских карт не допускается.

---

4. Использование платёжных провайдеров

Для обработки платёжных данных используются сертифицированные платёжные провайдеры, соответствующие требованиям стандарта PCI DSS.

При этом:

- ввод реквизитов карты осуществляется на стороне платёжного провайдера
- сайт не получает и не хранит полные реквизиты карты
- применяется токенизация платёжных данных

---

5. Шифрование данных

Передача данных осуществляется с использованием современных криптографических протоколов:

- TLS версии не ниже 1.2
- шифрование данных при передаче (in transit)

При необходимости также применяется шифрование данных на стороне платёжного провайдера.

---

6. Аутентификация и дополнительные меры защиты

Для подтверждения операций могут использоваться:

- технология 3-D Secure (например, одноразовые коды банка)
- двухфакторная аутентификация
- системы предотвращения мошенничества (anti-fraud)

---

7. Ограничения и запреты

В целях обеспечения безопасности запрещается:

- передавать реквизиты карты по незащищённым каналам
- хранить CVV/CVC коды
- запрашивать полные реквизиты карты вне защищённой платёжной страницы
- передавать данные третьим лицам, не участвующим в обработке платежа

---

8. Ответственность и информирование

Пользователям рекомендуется:

- не передавать данные карты третьим лицам
- использовать только защищённые страницы оплаты
- проверять наличие HTTPS и корректность домена

В случае возникновения подозрений на компрометацию данных необходимо незамедлительно обратиться в банк-эмитент карты.

---

9. Заключительные положения

Передача конфиденциальной информации Держателей осуществляется с соблюдением требований действующего законодательства и международных стандартов безопасности платёжных систем