УГРОЗЫ БЕЗОПАСНОСТИ И СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТА ПРИ ОСУЩЕСТВЛЕНИИ QR ПЛАТЕЖЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Боложко П.А., Игнатчик Д.С.

Белоусова Е.С. – канд. техн. наук, доцент

Использование QR-кодов в повседневной жизни облегчают пользователям доступ к данным с помощью любого современного устройства с камерой. При этом возникают вопросы обнаружения уязвимостей использования QR-кодов, а также обеспечения безопасности транзакций.

Суть технологии QR (Quick Response Code) заключается в ее совместимости с сервисом SmartPay, которое может быть, как банковским, так и коммерческим. Установив приложение на устройство и осуществив выбор товаров, покупатель может оплатить их QR-платежом. После открытия приложения и получения уникального QR-кода устройство необходимо приложить к сканеру, и оплата будет реализована. В приложение покупатель получит электронный чек. Проблема в том, что отличить QR-код магазина от QR-кода злоумышленника на глаз невозможно. Если торговая точка использует статический код, киберпреступник может просто заклеить его своим. Для этого ему необходимо создать QR-код с личным счетом, используя приложения-генераторы, которые находятся в открытом бесплатном доступе.

На основе проведенных исследований нами предложено два основных типа возможных мер по нейтрализации угроз при осуществлении QR-платежей: социально-психологические меры и инженерно-технические, основанные на использовании специального программного обеспечении (ПО).

В качестве социально-психологических мер предлагаются следующие:

– проверка суммы оплаты и ее получателя перед подтверждением транзакции;

– проверка легитимности код (не наклеен ли он поверх другого);

– генерирация платёжного кода непосредственно в момент оплаты.

В качестве специального ПО мы факультативно разрабатываем программу «предаутентицификации продавца», принцип которой основан на использовании стандарта EMVCo для платежей с помощью QR (рисунок 1).

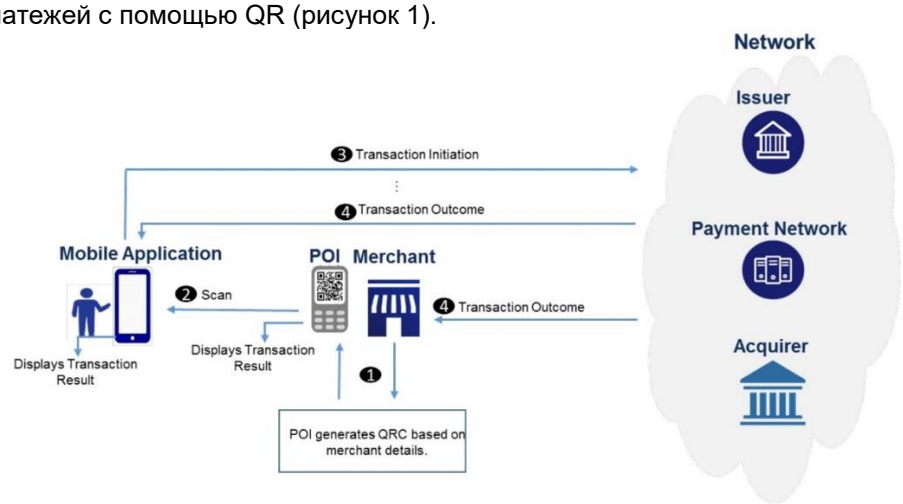

Рисунок 1 – Стандарт EMVCo для QR-платежей

После сканирования данных информация о транзакции дублируется и передаётся на выделенный сервер, где проходит обработку и сопоставляется с открытой банковской базой данных юридических лиц. В случае успешного сравнения и получения одобрения от сервера копия информации о транзакции идёт далее по представленной на рисунке 1 схеме. В случае неодобрения транзакция прерывается и информация отправляется в FINCert Национального Банка Республики Беларусь. Таким образом, правильная и эффективная работа данной системы возможна только при консолидации всех субъектов банковской сферы Республики Беларусь.

Список использованных источников:
Оплата по QR коду - https://www.raschet.by/platelshchikam/ais-raschet/oplata-po-qr-kodu/
Опыт Китая по созданию расчетного пространства и оплате QR-кодами - https://www.hutkigrosh.by/blog/oplataqrkodami/
QR-коды — от Японии до России - https://www.kaspersky.ru/blog/qr-code-payments/22960/