Банк России

СТАНДАРТ БАНКА РОССИИ

СТО БР БФБО-1.9-2024

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ QR-КОДОВ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

Москва
2024

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Принят и введен в действие приказом Банка России от 28.12.2024 № ОД-2367.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту, о пересмотре (замене) или об отмене стандарта размещается на сайте Банка России в сети Интернет (http://www.cbr.ru/).

ВВЕДЕНИЕ

Настоящий стандарт разработан для унификации видов и способов безопасного применения QR-кодов при осуществлении переводов денежных средств и позволяет решить следующие задачи:

- выделение технологических участков и подэтапов процессов осуществления переводов денежных средств с использованием QR-кодов;
- определение риска информационной безопасности на технологических участках и подэтапах указанных выше процессов, актуальных угроз безопасности информации и мер защиты информации для снижения выявленного риска;
- стандартизация взаимодействия участников указанных выше процессов при осуществлении переводов денежных средств с использованием QR-кодов;
- внедрение единых правил формирования и использования QR-кодов в процессах осуществления переводов денежных средств на основе международных стандартов.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт рекомендован к использованию при осуществлении деятельности, направленной на обеспечение безопасности использования статических и динамических QR-кодов для совершения переводов денежных средств.

Положения настоящего стандарта предназначены для использования кредитными организациями, некредитными финансовыми организациями, операторами платежных систем, операционным и платежным клиринговым центром Системы быстрых платежей и иными организациями, участвующими в осуществлении переводов денежных средств с использованием QR-кодов, поставщиками платежных приложений, прикладного программного обеспечения, информационных систем, электронных средств платежа (далее при совместном упоминании – организации), которые применяются для инициации и совершения переводов денежных средств с использованием QR-кодов.

Настоящий стандарт определяет:

- технологические участки инициации и совершения переводов денежных средств с использованием QR-кодов;
- принципы и этапы процесса формирования данных для QR-кодов в автоматизированных системах поставщиков платежных приложений, прикладного программного обеспечения, информационных систем, электронных средств платежа, которые применяются для инициации и совершения переводов денежных средств с использованием QR-кодов;
- способы использования данных, необходимых для формирования QR-кодов в автоматизированных системах поставщиков платежных приложений, прикладного программного обеспечения, информационных систем, электронных средств платежа, которые применяются для инициации и совершения переводов денежных средств с использованием QR-кодов;
- способы преобразования данных в QR-код плательщиком/получателем, полученных от поставщика платежного QR-кода;
- способы представления QR-кода плательщиком/получателем для осуществления переводов денежных средств;
- меры защиты на технологических участках и подэтапах осуществления переводов денежных средств с использованием QR-кодов;
- сценарии использования QR-кодов при выполнении переводов денежных средств.

Настоящий стандарт предназначен для применения в организациях при реализации процессов осуществления переводов денежных средств с использованием статических и динамических QR-кодов, формируемых:

- плательщиком – для предоставления получателю реквизитов плательщика, в том числе платежных ссылок;
- получателем – для предоставления плательщику реквизитов получателя или платежной ссылки.

Положения настоящего стандарта носят рекомендательный характер, если только обязательность применения некоторых из них не установлена нормативными правовыми актами, в том числе нормативными актами Банка России. Настоящий стандарт может быть использован для включения ссылок на него и (или) для прямого включения содержащихся в нем положений во внутренние документы организаций финансового рынка, а также в договоры, заключенные между организациями.

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использованы нормативные ссылки на следующие документы:

1. Национальный стандарт Российской Федерации ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 07.08.2012 № 216-ст) (далее – ГОСТ Р 34.11-2012).

2. Национальный стандарт Российской Федерации ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 19.06.2015 № 749-ст) (далее – ГОСТ Р 34.12-2015).

3. Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 822-ст) (далее – ГОСТ 57580.1-2017).

4. Стандарт Банка России СТО БР БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» (принят и введен в действие приказом Банка России от 01.03.2023 № ОД-335) (далее – СТО БР БФБО-1.7-2023).

5. Стандарт Банка России СТО БР БФБО-1.8-2024 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации» (принят и введен в действие приказом Банка России от 28.02.2024 № ОД-326) (далее – СТО БР БФБО-1.8-2024).

3. ПОРЯДОК ПРИМЕНЕНИЯ

Настоящий стандарт развивает положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» в части обеспечения защиты информации при осуществлении переводов денежных средств с использованием QR-кодов [1], [2].

В стандарте рассматриваются меры по обеспечению защиты QR-кодов и контроля информационной безопасности при их применении, специфические для переводов денежных средств с использованием QR-кодов на технологических участках «Формирование (подготовка), передача и прием электронных сообщений», «Удостоверение права клиентов распоряжаться денежными средствами» и «Осуществление банковской операции, учет результатов ее осуществления», а также на подэтапе «Формирование (подготовка), передача и прием QR-кода» технологического участка «Формирование (подготовка), передача и прием электронных сообщений».

Настоящий стандарт также определяет виды QR-кодов, которые используются организациями, угрозы и меры защиты в целях обеспечения безопасности информации ограниченного доступа, необходимой для осуществления переводов денежных средств с использованием QR-кодов.

Организации при использовании положений настоящего стандарта и внедрении мер защиты, направленных на минимизацию риска информационной безопасности, также должны руководствоваться моделью угроз безопасности информации, разработанной в таких организациях. Для выбора необходимых мер защиты организациям целесообразно определить актуальность представленных в настоящем стандарте угроз применимо к своим процессам, связанным с осуществлением переводов денежных средств с использованием QR-кодов. При актуальности угроз организациям рекомендуется внедрить меры защиты, минимизирующие риск реализации соответствующих угроз. В случае неактуальности угроз, применимых к процессам организации, указанные в стандарте меры защиты не подлежат внедрению.

Настоящий стандарт включает приложения, в которых отражены способы представления QR-кодов для осуществления переводов денежных средств, состав данных QR-кода, схемы и описания различных процессов осуществления переводов денежных средств с использованием QR-кодов.

4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем стандарте применены следующие термины:

4.1

Банк плательщика: кредитная организация (или ее филиал), обслуживающая (обслуживающий) счет плательщика.

4.2

Банк получателя: кредитная организация (или ее филиал), обслуживающая (обслуживающий) счет получателя.

4.3

Банк пользователя: кредитная организация (или ее филиал), обслуживающая (обслуживающий) счет пользователя.

4.4

Операция СБП B2B: операция СБП, осуществляемая при переводе денежных средств от плательщика – юридического лица, индивидуального предпринимателя получателю – юридическому лицу, индивидуальному предпринимателю (за исключением переводов по поручению или в пользу юридических лиц, лицевые счета которых открыты в территориальных органах Федерального казначейства).
[3], раздел 1.2

4.5

Операция СБП C2B: операция СБП, осуществляемая при переводе денежных средств от плательщика – физического лица получателю – юридическому лицу, индивидуальному предпринимателю или самозанятому гражданину.
[3], раздел 1.2

4.6

Платежная ссылка: URL-адрес, который ведет на ресурс с данными, необходимыми для осуществления платежной операции.

4.7

Платежное приложение: предоставляемое поставщиком платежного приложения программное обеспечение на подключенном к информационно-телекоммуникационной сети «Интернет» техническом устройстве (включая смартфон, планшетный компьютер), позволяющее клиенту оператора по переводу денежных средств составлять и передавать распоряжения в целях осуществления перевода денежных средств с использованием электронного средства платежа.
[4], пункт 30 статьи 3

4.8

Плательщик: сторона (физическое лицо, индивидуальный предприниматель, юридическое лицо), которая переводит денежные средства.

4.9

Получатель: сторона (физическое лицо, индивидуальный предприниматель, юридическое лицо), в пользу которой переводят денежные средства.

4.10

Пользователь: сторона (физическое лицо, индивидуальный предприниматель, юридическое лицо), которая использует банкомат кредитной организации для списания/зачисления наличных денежных средств на счет.

4.11

Поставщик платежного приложения: юридическое лицо, в том числе иностранная организация, предоставляющее на основании договора с оператором по переводу денежных средств платежное приложение для его применения клиентами оператора по переводу денежных средств.
[4], пункт 29 статьи 3

4.12

Поставщик платежного QR-кода: организация, оказывающая услугу формирования QR-кода для перевода денежных средств получателю (например, кредитная организация, выполняющая функции банка получателя средств или банка плательщика, операционный и платежный клиринговый центр Системы быстрых платежей, поставщик электронного средства платежа, сторонние сервисы по формированию QR-кодов).

4.13

Строка: данные плательщика/получателя, представленные в формате Base64, для последующего преобразования в QR-код.

4.14

Техническое устройство: мобильное устройство, стационарный компьютер или иное устройство, используемое для отображения QR-кода плательщиком/получателем с целью осуществления платежных операций.

4.15

Токенизированная (цифровая) карта: преобразованные реквизиты платежной карты.

4.16

Электронное сообщение: сообщение, содержащее распоряжение о переводе денежных средств в электронном виде.

4.17

Электронное средство платежа: средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.
[4], пункт 19 статьи 3

5. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

ДБО – дистанционное банковское обслуживание

ОПКЦ СБП – операционный и платежный клиринговый центр Системы быстрых платежей

ПО – программное обеспечение

СБП – Система быстрых платежей

СиП – сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств

ТСП – торгово-сервисное предприятие

ФиП – формирование и представление QR-кода плательщиком/получателем

ФППЗ – формирование, передача и прием запроса (данных) для генерации QR-кода

ЮЛ – юридическое лицо

ЭСП – электронное средство платежа

MAC – message authentication code (код аутентификации сообщения)

POS – Point of Sale (место продажи)

TLS – transport layer security (протокол защиты транспортного уровня)

QR – Quick Response (быстрый отклик)

URL – Uniform Resource Locator (унифицированный указатель ресурса)

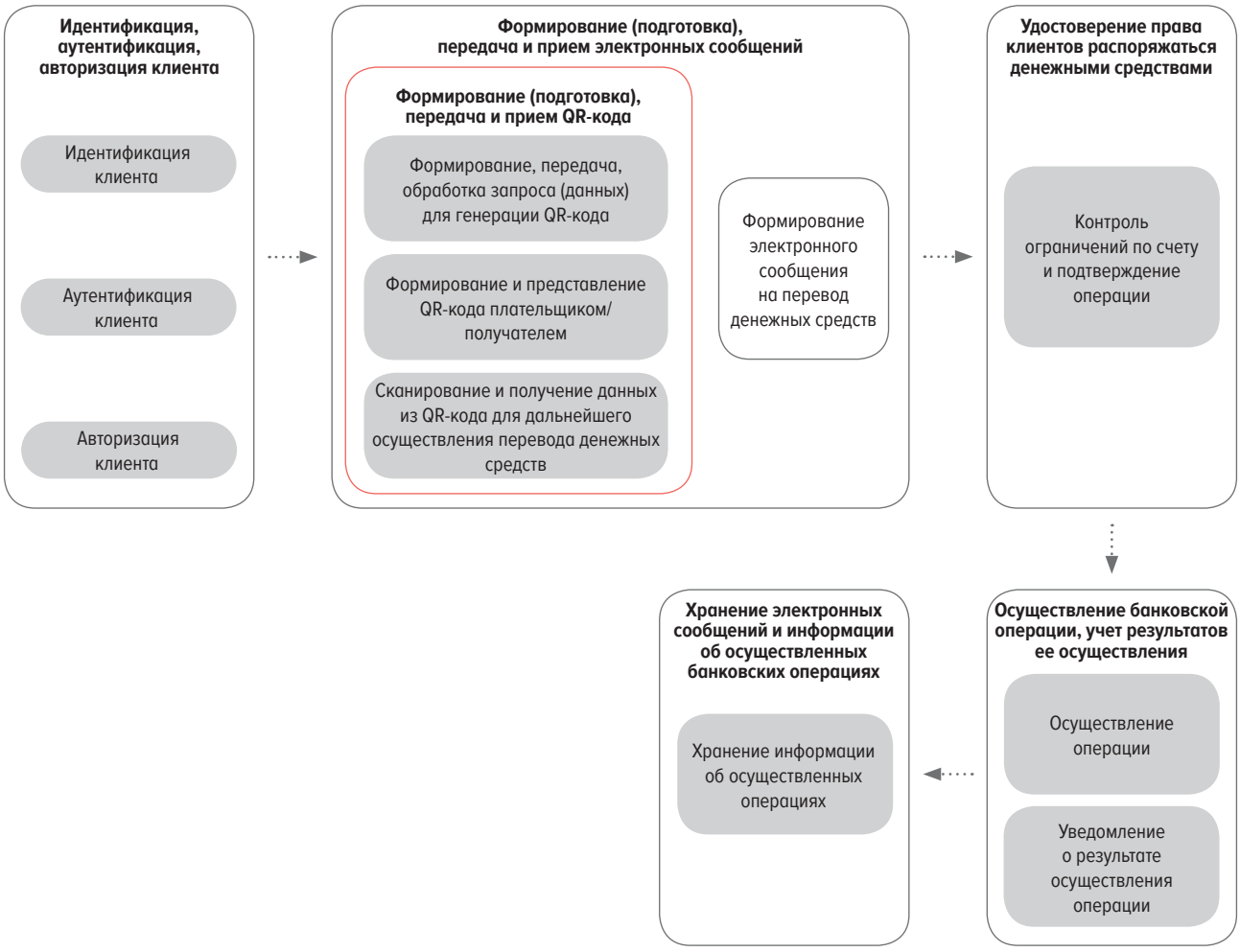
6. ОПИСАНИЕ ТЕХНОЛОГИЧЕСКИХ УЧАСТКОВ И ЭТАПОВ

Процесс осуществления переводов денежных средств разделен на следующие технологические участки, определенные в нормативных актах Банка России [1], [2]:

- идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций[1];
- формирование (подготовка), передача и прием электронных сообщений;
- удостоверение права клиентов распоряжаться денежными средствами;
- осуществление банковской операции, учет результатов ее осуществления;
- хранение электронных сообщений и информации об осуществленных банковских операциях.

Процесс формирования QR-кода для осуществления переводов денежных средств реализован на подэтапе «Формирование (подготовка), передача и прием QR-кода» технологического участка «Формирование (подготовка), передача и прием электронных сообщений» и представлен на рис. 1.

ТЕХНОЛОГИЧЕСКИЕ УЧАСТКИ И ШАГИ ПРОЦЕССА ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ИСПОЛЬЗОВАНИИ QR-КОДА *Рис. 1*



[1] Полное название технологического участка указано в абзаце втором подпункта 5.2 пункта 5 Положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

На подэтапе «Формирование (подготовка), передача и прием QR-кода» выделяются следующие шаги:

- формирование, передача, обработка запроса (данных) для генерации QR-кода; этот шаг включает формирование получателем QR-кода запроса с данными, необходимыми для генерации QR-кода, его передачу по каналам связи поставщику платежного QR-кода, прием поставщиком платежного QR-кода такого запроса с данными, обработка и формирование строки с данными / со ссылкой и ее последующая передача получателю;
- формирование и представление QR-кода плательщиком/получателем; этот шаг включает обработку плательщиком/получателем строки с данными / ссылки, полученной от поставщика платежного QR-кода и преобразование ее в графический вид для представления получателю/ плательщику;
- сканирование и получение данных из QR-кода для дальнейшего перевода денежных средств; этот шаг включает сканирование плательщиком/получателем представленного QR-кода и получение из него данных/ссылки для дальнейшей обработки.

7. ВИДЫ И СПОСОБЫ ПРИМЕНЕНИЯ QR-КОДОВ В ПРОЦЕССАХ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

Существуют четыре типа платежных QR-кодов в зависимости от состава хранимой информации:

- QR-код с реквизитами плательщика – QR-код, сформированный плательщиком, в котором содержится информация, необходимая для совершения перевода денежных средств (например, реквизиты карты или счета);
- QR-код со ссылкой плательщика – QR-код с платежной ссылкой, сформированной поставщиком платежного QR-кода и перенаправляющей на ресурс с целевыми данными, необходимыми для совершения перевода денежных средств (например, реквизиты карты или счета);
- QR-код с реквизитами получателя – QR-код, сформированный получателем/поставщиком платежного QR-кода, в котором содержатся данные, необходимые для перевода денежных средств (информация об операции), либо платежные реквизиты получателя;
- QR-код со ссылкой получателя – QR-код с платежной ссылкой, сформированной поставщиком платежного QR-кода и перенаправляющей на ресурс с целевыми данными, необходимыми для совершения перевода денежных средств (например, реквизиты карты или счета).

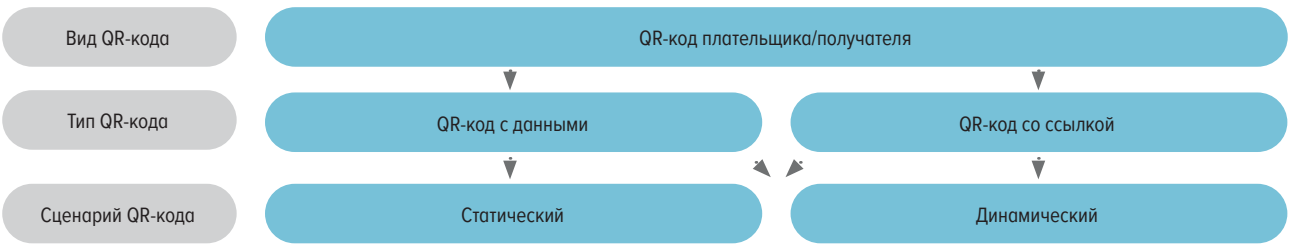
Платежные QR-коды могут использоваться в двух сценариях:
- динамический – код, который формируется для конкретной операции осуществления перевода денежных средств и содержит данные для перевода денежных средств (динамический QR-код);
- статический – код, который формируется однократно для регулярного использования при осуществлении операций по переводу денежных средств и содержит как платежную ссылку, так и реквизиты плательщика/получателя (статический QR-код).

На устройствах (носителях) платежные QR-коды могут быть представлены в двух вариантах отображения:
- онлайн – QR-коды генерируются непосредственно в момент оплаты в точке взаимодействия плательщика и получателя и представляются на устройствах плательщика/получателя;
- офлайн – QR-коды генерируются заранее, сохраняются на устройствах плательщика/получателя и представляются на таких устройствах в точке взаимодействия при необходимости.

QR-коды могут быть отображены на следующих устройствах (носителях):
- бумага/наклейка и иной способ физического представления графического изображения;
- веб-сайт (в частности, интернет-магазин и иные способы отображения в графическом виде в среде Интернет);
- различные POS-устройства;
- банкомат;
- иные технические устройства.

На рис. 2 представлены варианты QR-кодов плательщика и получателя, рассматриваемые в стандарте, которые могут применяться при осуществлении переводов денежных средств.

QR-КОДЫ ПЛАТЕЛЬЩИКА И ПОЛУЧАТЕЛЯ *Рис. 2*



Состав данных QR-кодов плательщика/получателя для функциональной совместимости при осуществлении переводов денежных средств рекомендуется реализовывать в соответствии с приложением 1 к настоящему стандарту.

8. СПОСОБЫ ПРЕДСТАВЛЕНИЯ QR-КОДОВ ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

Раздел является справочным. Схемы взаимодействия участников при формировании QR-кода могут отличаться от схем, представленных в настоящем стандарте.

QR-коды могут быть представлены для последующего сканирования и оплаты плательщиком или получателем.

При представлении QR-кода плательщиком с использованием ЭСП / платежного приложения на устройстве формируется запрос и передается поставщику платежного QR-кода. Поставщик платежного QR-кода возвращает плательщику в ЭСП / платежное приложение для преобразования в графический QR-код либо строку с данными, либо строку с платежной ссылкой.

Плательщик представляет QR-код получателю для сканирования и последующего осуществления перевода денежных средств [5], [7]. На рис. 3 представлена общая схема процесса формирования платежного QR-кода плательщиком.

Поставщиком платежного QR-кода для плательщика могут быть банк плательщика или поставщик платежного приложения.

Частные схемы процесса формирования QR-кода плательщиком могут быть реализованы в соответствии с разделом 1 приложения 2.

ФОРМИРОВАНИЕ QR-КОДА ПЛАТЕЛЬЩИКОМ *Рис. 3*

При представлении QR-кода получателем на устройстве в приложении формируется и передается запрос поставщику платежного QR-кода. Поставщик платежного QR-кода возвращает в приложение получателя строку с данными / со ссылкой для преобразования в графический QR-код. Получатель представляет QR-код плательщику для сканирования и последующего осуществления перевода денежных средств [6], [7]. На рис. 4 представлена общая схема процесса формирования платежного QR-кода получателем.

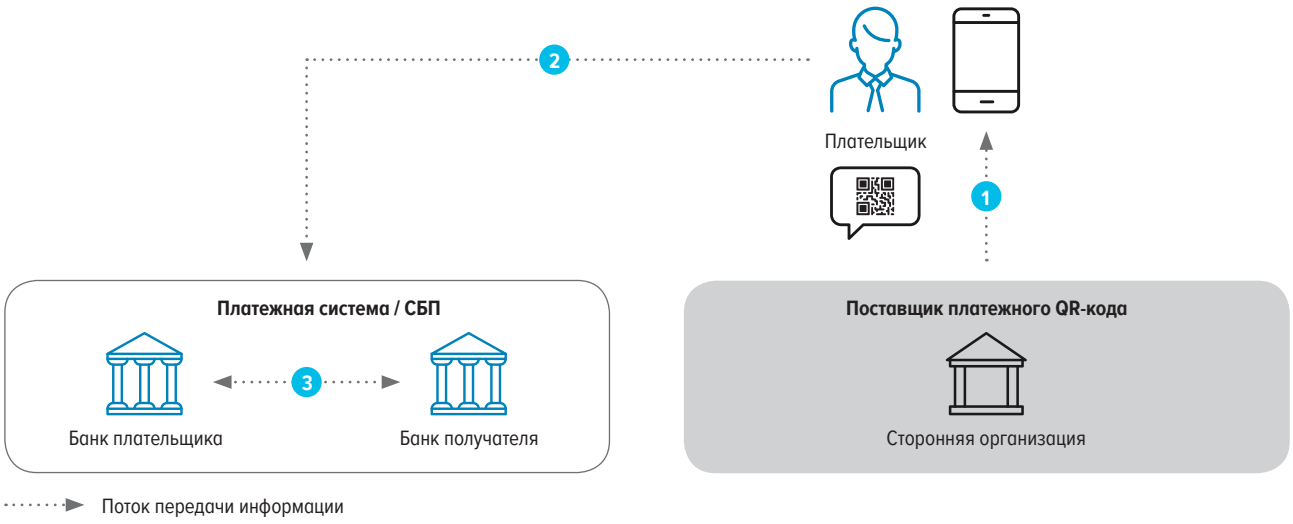
Поставщиком платежного QR-кода для получателя могут быть банк получателя, поставщик платежного приложения, ОПКЦ СБП.

ФОРМИРОВАНИЕ QR-КОДА ПОЛУЧАТЕЛЕМ *Рис. 4*

При представлении QR-кода получателем в прикладном ПО формируется QR-код с реквизитами получателя и печатается в квитанции. Получатель представляет плательщику квитанцию с QR-кодом для сканирования и последующего осуществления перевода денежных средств.

Поставщиком платежного QR-кода может быть сторонняя организация, которая использует для формирования QR-кода прикладное ПО.

ФОРМИРОВАНИЕ QR-КОДА ПОЛУЧАТЕЛЕМ (СТОРОННЕЙ ОРГАНИЗАЦИЕЙ) *Рис. 5*



Частные схемы процесса формирования QR-кода получателем могут быть реализованы в соответствии с разделом 2 приложения 2.

9. БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ QR-КОДОВ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

9.1. Общие положения

В соответствии с процессами, определенными на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода», в 9.2 обозначены типовые угрозы, реализуемые на данном подэтапе, для каждого типа QR-кода в статическом и динамическом сценариях.

В 9.3 обозначены меры защиты, актуальные для каждой угрозы, реализуемой на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода».

9.2. Типовые угрозы при осуществлении переводов денежных средств с использованием QR-кодов

Угрозы безопасности информации при осуществлении переводов денежных средств с использованием QR-кодов – это различные действия, которые могут привести к нарушению процессов осуществления переводов денежных средств, используя уязвимости, которыми обладают процессы и технические средства работы с QR-кодами. Реализация угрозы безопасности информации заключается в нарушении конфиденциальности, целостности и доступности информации, необходимой для совершения переводов денежных средств с использованием QR-кодов. При этом злоумышленник может предпринимать действия по модификации, уничтожению, блокированию информации, используемой в процессах переводов денежных средств.

Технологический подэтап «Формирование (подготовка), передача и прием QR-кода» разделен на три шага, на которых реализуются типовые угрозы для QR-кодов с данными и QR-кодов со ссылкой в статическом и динамическом сценариях. В табл. 1 представлены шаги на технологическом подэтапе, угрозы для каждого шага и их подробное описание, способы представления QR-кодов, объекты воздействия угроз, а также QR-коды, для которых актуальны такие угрозы.

Номер пункта таблицы соответствует шагу на технологическом подэтапе и угрозе и разделяется точкой. Следовательно, первая цифра пункта таблицы соответствует шагу на технологическом подэтапе, вторая – угрозе для этого шага на технологическом подэтапе. Например, номер 1.1, где согласно табл. 1 первая цифра – шаг «Формирование, передача и прием запроса (данных) для генерации QR-кода», а вторая – номер угрозы («Угроза модификации запроса на формирование QR-кода»).

ТИПОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ В ПРОЦЕССАХ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ QR-КОДОВ *Табл. 1*

№ п/п	Шаг на технологическом подэтапе (индекс)	Наименование угрозы	Описание угрозы	Представление QR-кода	Объект воздействия	Тип QR-кода			
						QR-код с данными		QR-код со ссылкой	
		Сценарии использования QR-кода				Статический	Динамический	Статический	Динамический
1.1	Формирование, передача и прием запроса (данных) для генерации QR-кода (ФППЗ)	Угроза модификации запроса на формирование QR-кода	Угроза заключается в возможности подмены реквизитов запроса на формирование QR-кода. Угроза возможна, если злоумышленник имеет доступ к одному из следующих процессов – формированию (подготовке), передаче, приему запроса	Получатель	Запрос на формирование QR-кода	+	+	+	+
				Плательщик		+	+	+	+
1.2		Угроза передачи неконтролируемых запросов на формирование QR-кода	Угроза обусловлена наличием несанкционированного доступа к АРМ ТСП, а также может быть вызвана ошибками прикладного ПО	Получатель	Сервис формирования данных для QR-кода	+	+	+	+
				Плательщик		+	+	+	+
1.3		Угроза модификации данных, содержащихся в запросе на формирование QR-кода	Угроза заключается в возможности злоумышленника модифицировать данные, используемые в запросе на формирование QR-кода. Угроза возможна, если злоумышленник имеет доступ к сервису формирования данных для QR-кода	Получатель	Сервис формирования данных для QR-кода; платежные реквизиты	+	+	+	+
				Плательщик		+	+	+	+
2.1	Формирование и представление QR-кода плательщиком/ получателем (ФиП)	Угроза модификации QR-кода при его формировании	Угроза заключается в возможности модификации QR-кода в процессе его преобразования в графический вид. Угроза возможна, если злоумышленник имеет доступ к сервису преобразования QR-кода в графический вид	Получатель	Алгоритм преобразования QR-кода в графический вид	+	+	+	+
				Плательщик		+	+	+	+
2.2		Угроза подмены QR-кода	Угроза заключается в подмене всего изображения QR-кода или подмене отдельных значений QR-кода злоумышленником	Получатель	QR-код	+	+	+	+
				Плательщик		+	+	+	+
2.3		Угроза кражи QR-кода плательщика	Угроза обусловлена возможностью злоумышленника похитить QR-код, сформированный плательщиком для получателя с целью совершения перевода денежных средств	Плательщик	QR-код	+	+	+	+
2.4		Угроза неконтролируемой передачи запросов на активацию QR-кода или ссылки	Угроза обусловлена наличием несанкционированного доступа к АРМ ТСП, а также может быть вызвана ошибками прикладного ПО или ошибочными действиями персонала	Получатель	Ресурс, на который ведет QR-код или платежная ссылка	-	-	+	+
				Плательщик		-	-	+	+
2.5		Угроза включения в QR-код избыточных данных	Угроза заключается в добавлении избыточных конфиденциальных данных в QR-код в открытом виде	Получатель	QR-код	+	+	+	+
				Плательщик		+	+	+	+

№ п/п	Шаг на технологическом подэтапе (индекс)	Наименование угрозы	Описание угрозы	Представление QR-кода	Объект воздействия	Тип QR-кода			
						QR-код с данными		QR-код со ссылкой	
		Сценарии использования QR-кода				Статический	Динамический	Статический	Динамический
3.1	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств (СиП)	Угроза повторного проведения перевода денежных средств	Угроза возможна, в случае если операция повторно проводится по одному и тому же QR-коду	Получатель	QR-код	+	+	+	+
				Плательщик		+	+	+	+
3.2		Угроза внедрения вредоносного кода (вызова удаленных процедур) с использованием QR-кода на устройстве плательщика	Угроза обусловлена отсутствием мер по контролю целостности данных (QR-кода), а также отсутствием мер по запрету на выполнение вызова удаленных процедур ЭСП / платежным приложением	Получатель	QR-код	+	+	+	+
				Плательщик		+	+	+	+
3.3		Угроза фишинга	Угроза заключается в перенаправлении плательщика/ получателя на сторонний сервис для выполнения операций, вследствие сканирования модифицированного злоумышленником QR-кода	Получатель	QR-код	+	+	+	+
				Плательщик		+	+	+	+
3.4		Угроза утечки конфиденциальных данных, содержащихся в QR-коде плательщика	Угроза обусловлена возможностью злоумышленника получить платежные данные, хранящиеся в QR-коде в открытом виде. Угроза актуальна для QR-кода с данными, сформированного плательщиком	Плательщик	QR-код	+	+	-	-

9.3. Типовые меры защиты информации при осуществлении переводов денежных средств с использованием QR-кодов

Применение QR-кодов является удобным способом для осуществления переводов денежных средств, который активно внедряется организациями. В связи с этим организации должны обеспечивать соответствующий уровень защиты информации при использовании QR-кодов в процессах переводов денежных средств для предотвращения мошенничества. В целях повышения безопасности процессов, в которых применяются QR-коды, необходимо применять определенные меры защиты информации, которые нейтрализуют типовые угрозы.

Меры, направленные на минимизацию угроз информационной безопасности, реализованные на подэтапе «Формирование (подготовка), передача и прием QR-кода», при использовании QR-кодов для осуществления переводов денежных средств отражены в табл. 2 [8], [9].

Номер меры защиты информации соответствует технологическому подэтапу, угрозе и мере защиты информации, которые разделяются точкой. Следовательно, первая цифра соответствует шагу на технологическом подэтапе / технологическому участку, вторая цифра – угрозе, которая может быть реализована, третья – мере защиты информации. Например, номер 1.1.1, где первая цифра является шагом «Формирование, передача и прием запроса (данных) для генерации QR-кода», вторая – номером угрозы («Угроза модификации запроса на формирование QR-кода»), третья – номером меры защиты («Контроль правильности заполнения полей запроса на формирование QR-кода»).

ТИПОВЫЕ МЕРЫ БЕЗОПАСНОСТИ В ПРОЦЕССАХ С ИСПОЛЬЗОВАНИЕМ QR-КОДОВ

Табл. 2

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Формирование, передача, обработка запроса (данных) для генерации QR-кода	1.1	1.1.1	Контроль правильности заполнения полей запроса на формирование QR-кода	Проведение контроля заполнения всех полей запроса, направляемого получателем/плательщиком поставщику платежного QR-кода в соответствии с требованиями настоящего стандарта	+	+
	1.1	1.1.2	Контроль целостности запроса на получение QR-кода (например, с использованием MAC)	Обеспечение целостности сообщений, содержащих запросы на генерацию QR-кода, с использованием криптографических алгоритмов, определенных национальными стандартами Российской Федерации	+	+
	1.1	1.1.3	Использование защищенного канала связи для передачи запроса на генерацию QR-кода	• Обеспечение защиты канала связи в соответствии с ГОСТ Р 34.12-2015 с использованием протокола TLS (с двухсторонней аутентификацией – при наличии технической возможности); или • обеспечение защиты канала связи на канальном или сетевом уровне с использованием средств криптографической защиты информации, прошедших оценку соответствия требованиям федерального органа исполнительной власти в области обеспечения безопасности	+	+
	1.1	1.1.5	Проверка полномочий на выполнение запроса формирования QR-кода	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных, с которых производится формирование и передача запроса на генерацию QR-кода в соответствии со стандартом Банка России СТО БР БФБО-1.7-2023	+	+
	1.2	1.2.1	Контроль на предмет отсутствия дублирования запросов (как исходящих, так и входящих) на формирование QR-кода	Осуществление контроля на предмет отсутствия дублирования запросов на формирование QR-кода перед отправлением и при приеме. Контроль происходит путем сверки уникального идентификатора запроса и идентификатора операции с уже имеющейся базой запросов на формирование QR-кодов или платежных ссылок	+	+
	1.2	1.2.2	Определение лимита запросов на формирование QR-кода	Определение лимитов запросов на формирование QR-кода с учетом потребностей получателя/плательщика и на основе анализа рисков поставщика платежного QR-кода	+	+

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Формирование, передача, обработка запроса (данных) для генерации QR-кода	1.3	1.3.1	Контроль значений реквизитов, помещаемых в QR-код или платежную ссылку, на соответствие значениям реквизитов платежа, полученным в запросе на генерацию QR-кода	Сравнение всех значений реквизитов, помещаемых в QR-код или платежную ссылку, со значениями, полученными в запросе на формирование QR-кода	+	+
	1.3	1.3.2	Обеспечение целостности данных запроса на формирование QR-кода (например, с использованием MAC) / применение механизмов и (или) протоколов передачи данных для формирования QR-кода, обеспечивающих защиту этих данных от искажения, фальсификации, переадресации	Обеспечение целостности данных, используемых для формирования и представления QR-кода, с использованием криптографических алгоритмов, определенных национальными стандартами Российской Федерации	+	+
	1.3	1.3.3	Использование защищенного канала связи при передаче запроса с данными, используемыми для формирования QR-кода	• Обеспечение защиты канала связи в соответствии с ГОСТ Р 34.12-2015 с использованием протокола TLS (с двухсторонней аутентификацией – при наличии технической возможности); или • обеспечение защиты канала связи на канальном или сетевом уровне с использованием средств криптографической защиты информации, прошедших оценку соответствия требованиям федерального органа исполнительной власти в области обеспечения безопасности	+	+
	1.3	1.3.4	Идентификация и аутентификация устройства, с которого передается запрос для формирования QR-кода	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных, с которых производится отправка данных для формирования QR-кода в соответствии со стандартом Банка России СТО БР БФБО-1.7-2023, а также национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017	+	+
	1.3	1.3.5	Обработка запросов на формирование QR-кода в системе, обрабатывающей запросы, соответствующей требованиям безопасности	Обеспечение соответствия системы поставщика платежного QR-кода, обрабатывающей запрос с данными для формирования QR-кода, требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017	+	+

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Формирование, передача, обработка запроса (данных) для генерации QR-кода	2.3	2.3.1	Формирование метки времени в зашифрованном виде, содержащейся в QR-коде, и ограничение времени жизни для данного QR-кода	• Добавление в QR-код метки времени по факту его формирования (или формирования данных для его генерации) с использованием односторонней хеш-функции, полученной в соответствии с ГОСТ Р 34.11-2012, или ключевой хеш-функции, основанной на использовании отечественных криптографических алгоритмов шифрования; • ограничение времени жизни динамического QR-кода, которое не превышает две минуты	+	+
	2.5	2.5.1	Ограничение на использование конфиденциальных данных в открытом виде в составе данных QR-кода	Контроль отсутствия конфиденциальной информации в составе данных QR-кода	+	+
	2.5	2.5.2	Разработка и утверждение внутреннего регламентирующего документа, где будет отражен состав данных, разрешенных для включения в QR-код	Утверждение внутреннего регламентирующего документа, в котором будет описан состав данных, разрешенный для включения в QR-код	+	+
	3.1	3.1.5	Установление лимита операций для статического QR-кода плательщика	Определение банком плательщика лимитов операций для статического QR-кода, необходимых для осуществления плательщиком переводов денежных средств, в соответствии с определенными в организации уровнями рисков	+	-
	3.4	3.4.1	Обезличивание данных плательщика/ получателя	• Применение технологии токенизации данных в QR-кодах; • минимизация использования конфиденциальных данных и данных, утечка которых может привести к осуществлению операций без добровольного согласия клиента, в динамических QR-кодах; • применение коротких ссылок, ведущих на защищенный ресурс, где находятся данные	+	+
	3.4	3.4.2	Защита от несанкционированного просмотра данных, получаемых при сканировании QR-кода	Использование алгоритмов шифрования данных, содержащихся в QR-коде для сокрытия реквизитов	+	+
	3.4	3.4.4	Ограничения по лимиту операций и сроку жизни QR-кода (актуально для QR-кода в статическом сценарии со ссылкой)	• Ограничение срока жизни QR-кода • Установление лимита по сумме	+	-

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Формирование и представление QR-кода плательщиком/ получателем	1.3	1.3.6	Контроль соответствия сформированной строки для QR-кода запросу на формирование	Обеспечение сверки ЭСП / платежным приложением плательщика и получателя полученной от поставщика платежного QR-кода строки с данными для преобразования в QR-код на соответствие отправленному запросу на формирование QR-кода	+	+
	2.1	2.1.1	Применение механизмов, обеспечивающих защиту алгоритмов преобразования QR-кода в графический вид для прикладного ПО (применение средств контроля целостности, обеспечение обновлений ПО из доверенного источника)	• Обеспечение контроля целостности ПО для преобразования QR-кода в графический вид (генератора QR-кода и среды его функционирования) средствами контроля целостности, имеющих сертификат соответствия ФСТЭК России; • проведение тестирования обновлений (интеграционное, функциональное) перед обновлением ПО, формирующего QR-код; • изоляция процесса (преобразования QR-кода в графический вид) в выделенной области памяти	+	+
	2.3	2.3.2	Аутентификация плательщика до отображения/преобразования строки в QR-код (графический вид)	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных, на которых отображается QR-код в соответствии со стандартом Банка России СТО БР БФБО-1.7-2023	+	+
	2.3	2.3.5	Установление по умолчанию запрета на скриншот экрана, где размещено изображение QR-кода плательщика, и на отображение экрана сторонним приложениям	Установка запрета на снимок экрана, где размещено изображение QR-кода	+	+
	2.4	2.4.1	Контроль на предмет отсутствия дублирования запросов на активацию ресурса, на который ведет QR-код или платежная ссылка	Осуществление контроля на предмет отсутствия дублирования запросов на активацию ресурса, на который ведет QR-код / платежная ссылка перед отправлением получателем и при приеме таких запросов поставщиком платежного QR-кода	+	-
	2.4	2.4.3	Ограничение возможности передачи запросов на активацию ресурса, на который ведет QR-код или платежная ссылка	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных, с которых передается запрос на активацию ресурса, на который ведет QR-код, в соответствии с рекомендациями стандарта Банка России СТО БР БФБО-1.7-2023	+	-

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1	2.1.2	Отображение реквизитов, содержащихся в QR-коде, плательщику для принятия решения по его использованию	Отображение плательщику реквизитов операции, полученных из QR-кода или платежной ссылки, предоставленных получателем платежа. Запрос подтверждения плательщика правильности заполненных реквизитов платежа	+	+
	2.2	2.2.1	Применение защитных механизмов при распечатывании статических QR-кодов, позволяющих пользователю заметить его подмену	• Использование визуальных эффектов (логотипов) для формирования отличительных признаков от обычных QR-кодов. Мера направлена на повышение сложности подделки QR-кода с визуальным эффектом; • использование голографических изображений на распечатанных QR-кодах	+	-
	2.2	2.2.3	Отображение реквизитов операции, содержащихся в QR-коде, плательщику для принятия решения по его использованию	Отображение реквизитов операции плательщику (например, ссылка на ресурс) и запрос на подтверждение действий	+	+
	2.2	2.2.4	Проверка данных из QR-кода, необходимых для формирования электронного сообщения	Проведение проверки целостности данных поставщиком платежного QR-кода, содержащихся в отсканированном QR-коде с использованием хеш-функции, сформированной по ГОСТ Р 34.11-2012, или ключевой хеш-функции, основанной на использовании отечественных криптографических алгоритмов шифрования	+	+
	3.2 3.3	3.2.1	Отображение реквизитов операции, содержащихся в QR-коде, плательщику для принятия решения по осуществлению операции	Отображение плательщику реквизитов операции, полученных из QR-кода или платежной ссылки. Запрос подтверждения плательщика о правильности заполненных реквизитов	+	+
	3.2 3.3	3.2.2	Использование средства защиты от вредоносного кода	• Встраивание в ЭСП / платежные приложения, обрабатывающие QR-код, модулей антивирусного ПО для проверки QR-кода на наличие вредоносного кода; • непрерывное обновление сигнатур баз данных приложений для сканирования QR-кодов; • подготовка рекомендаций и информирование плательщиков по использованию антивирусного ПО; • внедрение процедур проверки содержимого QR-кода, в том числе проверка URL-адреса короткой ссылки по спискам вредоносных ссылок	+	+
	3.2 3.3	3.2.3	Внедрение процедур проверки QR-кода в ПО	Внедрение процедуры проверки подлинности QR-кода	+	+

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1	1.1.4	Проверка полномочий на выполнение запроса формирования QR-кода	• Идентификация и аутентификация плательщика/получателя при входе в ЭСП / при входе в мобильное устройство для доступа к платежному приложению; • запрет действий плательщика/получателя до идентификации и аутентификации в ЭСП / платежном приложении; • запрет действий плательщика/получателя до идентификации и аутентификации в ЭСП / на мобильном устройстве для доступа к платежному приложению	+	+
	2.3	2.3.2	Аутентификация плательщика до отображения/преобразования строки в QR-код (графический вид)	• Идентификация и аутентификация плательщика в ЭСП / платежном приложении, отображающем QR-код; • запрет действий плательщика по использованию QR-кода до проведения идентификации и аутентификации в ЭСП / платежном приложении	+	+
	2.4	2.4.3	Ограничение возможности передачи запросов на активацию ресурса, на который ведет QR-код или платежная ссылка	• Идентификация и аутентификация пользователей, являющихся работниками получателя, при входе в приложение; • запрет действий получателя до идентификации и аутентификации в приложении	+	-
Формирование (подготовка), передача и прием электронных сообщений	3.1	3.1.6	Контроль дублирования данных и операции перевода денежных средств	Присвоение банком плательщика уникального идентификатора для каждой операции осуществления перевода денежных средств, проводимой с использованием QR-кода	+	+
Удостоверение права клиентов распоряжаться денежными средствами	1.1	1.1.6	Использование геометок для динамических QR-кодов	Поставщик платежного QR-кода проверяет местонахождение получателя/плательщика (при наличии/возможности сбора информации о географическом местоположении) во время обработки платежа. Геометка, полученная в запросе на создание QR-кода, должна совпадать с геометкой, направляемой в ЭС	-	+
	2.3	2.3.4	Установление лимита операций для QR-кода плательщика	Лимиты платежей и лимиты суммы платежей для QR-кода определяются внутренними регламентирующими документами поставщика платежного QR-кода на основании анализа рисков	+	+
	2.3	2.3.7	Подтверждение операции по QR-коду плательщиком	Подтверждение операции плательщиком в ЭСП / платежном приложении с использованием дополнительных факторов аутентификации в соответствии со СТО БР БФБО-1.8-2024	+	+
	3.1	3.1.4	Осуществление антифрод-мероприятий	Антифрод-мероприятия проводятся в соответствии с уровнями риска, определенными банком плательщика, банком получателя для переводов денежных средств	+	+

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Удостоверение права клиентов распоряжаться денежными средствами	3.1	3.1.5	Установление лимита операций для статического QR-кода плательщика	Определение банком плательщика лимитов для операций со статическим QR-кодом, необходимых для осуществления плательщиком переводов денежных средств, в соответствии с определенными в организации уровнями рисков	+	-
Осуществление банковской операции, учет результатов ее осуществления	3.1	3.1.1	Деактивация ресурса, на который ведет короткая ссылка из QR-кода, после завершения платежа (актуально для QR-кода в статическом сценарии со ссылкой)	Ресурс, на который ведет короткая ссылка из QR-кода, может быть использован только один раз (то есть деактивироваться сразу после совершения перевода денежных средств)	+	-
	3.1	3.1.2	Применение уникального идентификатора для каждой операции	Присваивание каждой операции, совершаемой с использованием QR-кода, уникального идентификатора в течение операционного дня	+	+
	3.1	3.1.3	Уничтожение динамического QR-кода после осуществления операции	Обеспечение уничтожения QR-кода плательщика/получателя в динамическом сценарии сразу после осуществления перевода денежных средств. Время жизни динамического QR-кода не должно превышать две минуты	-	+
	3.1	3.1.7	Контроль дублирования данных и операции перевода денежных средств	Обеспечение проверки банком плательщика на предмет дублирования данных операции по переводу денежных средств, которая происходит на основании данных из QR-кода	+	+
	3.1	3.1.8	Уведомление о совершенной операции по QR-коду	Обеспечение передачи уведомления плательщику о списании денежных средств по операции с использованием QR-кода. Обеспечение передачи уведомления получателю о зачислении денежных средств по операции с использованием QR-кода	+	+
	3.4	3.4.3	Деактивация ресурса, на который ведет ссылка из QR-кода после осуществления операции (актуально для QR-кода в динамическом сценарии со ссылкой)	Использование процесса деактивации ресурса, на который ведет ссылка из QR-кода, после осуществления перевода денежных средств	-	+

Шаг на технологическом подэтапе / технологический участок	№ угрозы	№ меры защиты	Наименование меры защиты	Описание меры защиты, возможная реализация	Сценарий QR-кода	
					Статический	Динамический
Все шаги технологического подэтапа / технологические участки	2.2	2.2.2	Разработка рекомендаций для пользователей по использованию QR-кодов	• Добавление в рекомендации правил использования, возможные риски использования QR-кодов, сканеров QR-кодов и меры по снижению рисков; • доведение рекомендаций по обеспечению безопасности QR-кодов понятным и доступным для пользователей образом (например, рекомендации могут быть в платежных приложениях в виде новостей)	+	+
	2.3	2.3.3	Учет рисков при осуществлении переводов денежных средств с использованием офлайн-QR-кода	Обеспечение учета рисков при осуществлении переводов денежных средств с использованием офлайн-QR-кода. Определение лимитов офлайн-операций в целом и лимитов суммы офлайн-операций с использованием QR-кода. Лимиты операций определяются внутренними регламентирующими документами поставщика платежного QR-кода	+	-
	2.3	2.3.6	Информирование владельца QR-кода через ЭСП / платежное приложение о необходимости обязательной блокировки операций по украденным QR-кодам	Информирование владельца QR-кода через ЭСП / платежное приложение о необходимости обязательной блокировки операций по украденным QR-кодам. Внесение в договор с клиентом информации о необходимости информирования банка плательщика о краже QR-кода	+	+
	2.4	2.4.2	Разработка рекомендаций и (или) требований для ТСП по обеспечению информационной безопасности для оборудования, обеспечивающего операции с использованием QR-кода	Разработка рекомендаций по информационной безопасности для ТСП при осуществлении операций с использованием QR-кодов, формируемых поставщиком платежного QR-кода. Социальная реклама и обучение работников ТСП, которые взаимодействуют с поставщиком платежного QR-кода	+	+
	3.2 3.3	3.2.4	Повышение уровня осведомленности плательщиков/получателей при использовании платежных QR-кодов	Подготовка обучающих материалов по безопасному использованию QR-кодов, различных сканеров QR-кодов для их распознавания, распространение среди плательщиков/получателей, использующих платежные QR-коды (например, публикация информации в платежных приложениях, ЭСП, СМИ, по телевидению)	+	+

ПРИЛОЖЕНИЕ 1. СОСТАВ ДАННЫХ QR-КОДА ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ

Для унификации процесса перевода денежных средств с использованием QR-кода рекомендуется соблюдать требования к символике, методам кодирования знаков данных, форматов символов, требования к размерам, правилам исправления ошибок, установленные стандартом ГОСТ Р ИСО/МЭК 18004-2015 [10].

При взаимодействии между плательщиком и получателем для осуществления переводов денежных средств выделяются два вида QR-кодов:

1. QR-код плательщика.

Поставщиком платежного QR-кода для плательщика являются:

- банк плательщика;
- поставщик платежного приложения.

При таком взаимодействии в QR-код включаются идентификационные данные плательщика, необходимые для осуществления перевода денежных средств. При этом данные для авторизационного запроса на перевод денежных средств формируются получателем в приложении после сканирования QR-кода плательщика и передаются вместе с данными плательщика в банк получателя средств, который отправляет запрос через платежную систему в банк плательщика для подтверждения возможности осуществления перевода денежных средств.

2. QR-код получателя.

Поставщиком платежного QR-кода для получателя являются:

- банк получателя;
- сторонняя организация;
- ОПКЦ СБП.

При таком взаимодействии в QR-код включаются идентификационные данные получателя (платежные реквизиты либо информация по операции), необходимые для совершения перевода денежных средств. Эти данные для осуществления перевода денежных средств после сканирования плательщиком QR-кода передаются из его ЭСП / платежного приложения в банк плательщика, который передает запрос для подтверждения возможности осуществления перевода денежных средств в банк получателя. При положительном результате проверок возможности зачисления денежных средств на счет получателя банк получателя возвращает в банк плательщика подтверждение осуществления перевода денежных средств. Банк плательщика списывает денежные средства со счета плательщика, банк получателя зачисляет денежные средства на счет получателя.

Для достижения функциональной совместимости QR-кодов всеми участниками процесса осуществления переводов денежных средств необходимо использовать унифицированный формат данных при формировании QR-кодов. QR-код с унифицированными данными, предоставляемыми плательщиком/получателем, должен приниматься всеми участниками процесса осуществления перевода денежных средств, поддерживаться техническим устройством плательщика, поддерживаться оборудованием получателя, а также банкоматами.

Для повышения конфиденциальности и уровня безопасности данных в процессах осуществления переводов денежных средств необходимо применять соответствующие меры защиты. Основным принципом повышения уровня безопасности данных в процессе перевода денежных средств

с использованием QR-кода является исключение применения чувствительных данных в открытом (незащищенном) виде при их формировании, обработке, передаче и хранении. Подробнее типовые угрозы и меры защиты данных описаны в разделе 9 настоящего стандарта.

Для достижения функциональной совместимости всеми участниками процессов осуществления переводов денежных средств в состав QR-кода рекомендуется включить следующие данные (в зависимости от вида QR-кода) [11]:

1. В QR-код плательщика с реквизитами – данные, необходимые для осуществления перевода денежных средств. При этом для данных плательщика рекомендовано реализовывать меры защиты, которые описаны в разделе 9 настоящего стандарта.

2. В QR-код получателя с реквизитами – следующие данные:
- реквизиты получателя, необходимые для осуществления перевода денежных средств. При этом для данных получателя рекомендовано реализовывать меры защиты, которые описаны в разделе 9 настоящего стандарта;
- логотип поставщика платежного QR-кода, который его сформировал для осуществления перевода денежных средств.

3. В QR-код со ссылкой плательщика/получателя – унифицированный указатель ресурса в виде URL-адреса.

Структура QR-кода для процесса перевода денежных средств в режиме представления плательщиком/получателем формируется в виде URL-адреса:

```
HTTPS://<ID Поставщика платежного QR-кода>/<ID QR-кода>/<Тип QR-кода>/<Сумма>/<Валюта>/<Контрольная сумма>
```

В табл. 1 представлены параметры, которые рекомендуется включать в состав URL-адреса при осуществлении переводов денежных средств с использованием QR-кодов.

ПАРАМЕТРЫ URL-АДРЕСА *Табл. 1*

№	Параметр	Описание	Тип данных
1.	ID поставщика платежного QR-кода	Включает сокращенное название поставщика платежного QR-кода, которое будет однозначно его идентифицировать	Строка
2.	ID QR-кода	Включает уникальный идентификатор QR-кода, который будет однозначно указывать на его принадлежность плательщику/получателю	Строка
3.	Тип QR-кода	Включает сценарий выполнения QR-кода. Может принимать значения: 01 – статический сценарий; 02 – динамический сценарий	Строка
4.	Сумма	Указывается сумма денежных средств в копейках	Строка
5.	Валюта	Указывается валюта операции, которая принимает значение «RUB»	Строка
6.	Контрольная сумма	Указывается контрольная сумма URL-адреса	Строка

В QR-код, предоставляемый получателем, рекомендовано включать логотип поставщика платежного QR-кода, который его сформировал для осуществления перевода денежных средств.

ПРИЛОЖЕНИЕ 2. СПОСОБЫ ПРЕДСТАВЛЕНИЯ QR-КОДОВ ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

1. Режим отображения плательщиком QR-кода, сформированного поставщиком платежного QR-кода

1.1. Поставщик платежного QR-кода – банк плательщика

Параметры QR-кода:

- Вид – QR-код плательщика.
- Тип – QR-код с данными средства платежа / QR-код со ссылкой.
- Сценарии формирования QR-кода:
  - статический для QR-кода с данными;
  - статический для QR-кода со ссылкой;
  - динамический для QR-кода с данными;
  - динамический для QR-кода со ссылкой.

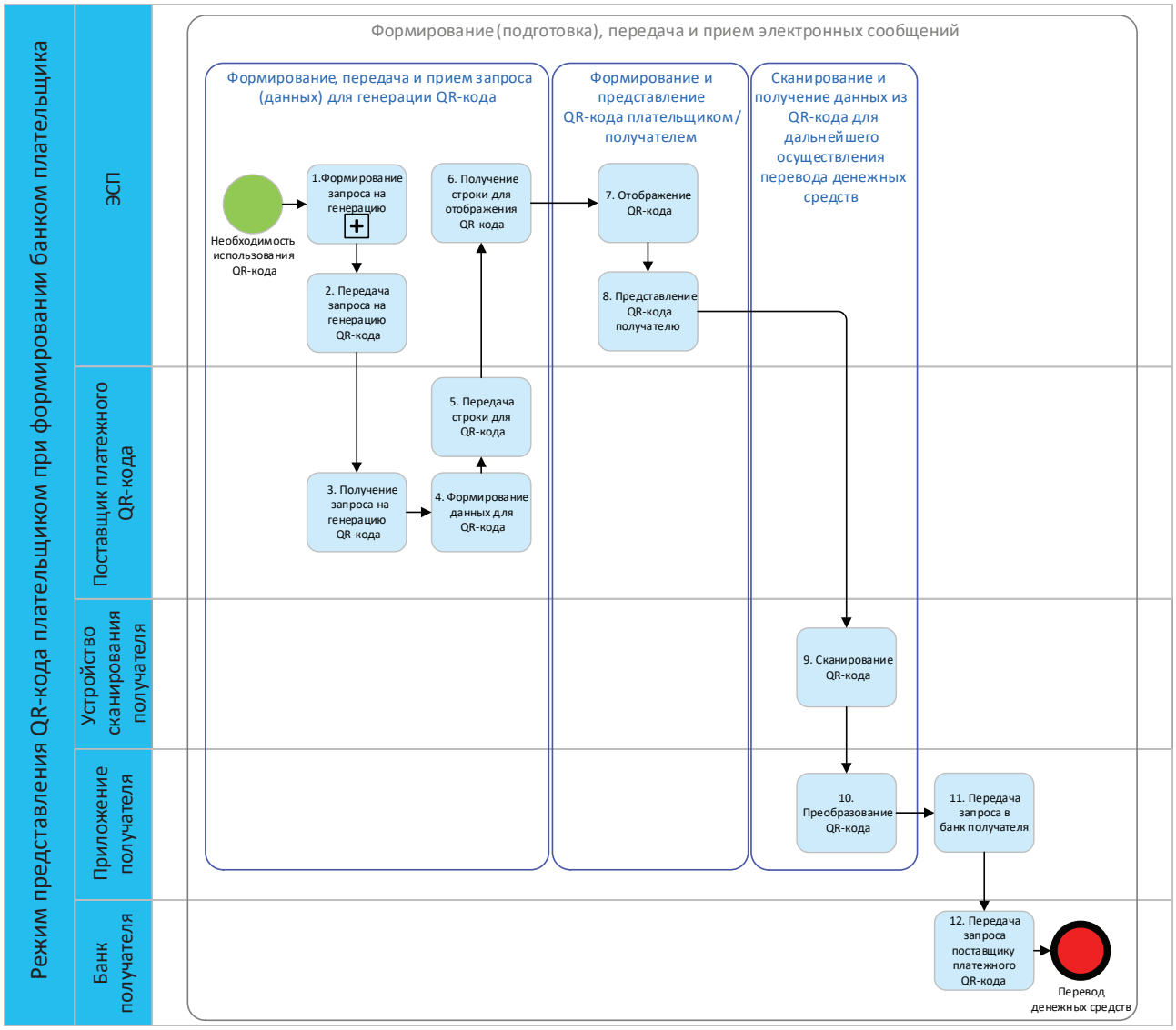
Базовые шаги процесса осуществления переводов денежных средств со сканированием QR-кода с данными в статическом/динамическом сценариях, представленного на устройстве плательщика, показаны на рис. 1.

ШАГИ ПРОЦЕССА ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ФОРМИРОВАНИИ QR-КОДА БАНКОМ ПЛАТЕЛЬЩИКА *Рис. 1*

Плательщик на устройстве формирует и передает запрос поставщику платежного QR-кода для формирования статического/динамического QR-кода. Поставщик платежного QR-кода возвращает на устройство плательщика строку с данными / со ссылкой для преобразования в графический QR-код. Плательщик представляет QR-код получателю. Получатель сканирует QR-код и передает авторизационный запрос с данными / со ссылкой из QR-кода в банк получателя. Далее денежные средства переводятся стандартным способом.

Схема процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода банком плательщика представлена на рис. 2.

ПРОЦЕССЫ ПОДЭТАПА «ФОРМИРОВАНИЕ (ПОДГОТОВКА), ПЕРЕДАЧА И ПРИЕМ QR-КОДА» ПРИ ФОРМИРОВАНИИ QR-КОДА БАНКОМ ПЛАТЕЛЬЩИКА *Рис. 2*



Описание схемы процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода банком плательщика для осуществления переводов денежных средств с представлением QR-кода плательщиком представлено в табл. 2.

Дополнительные схемы с использованием QR-кода плательщика при формировании банком плательщика для сканирования получателем с помощью сканера приведены в приложениях 4, 5 настоящего стандарта.

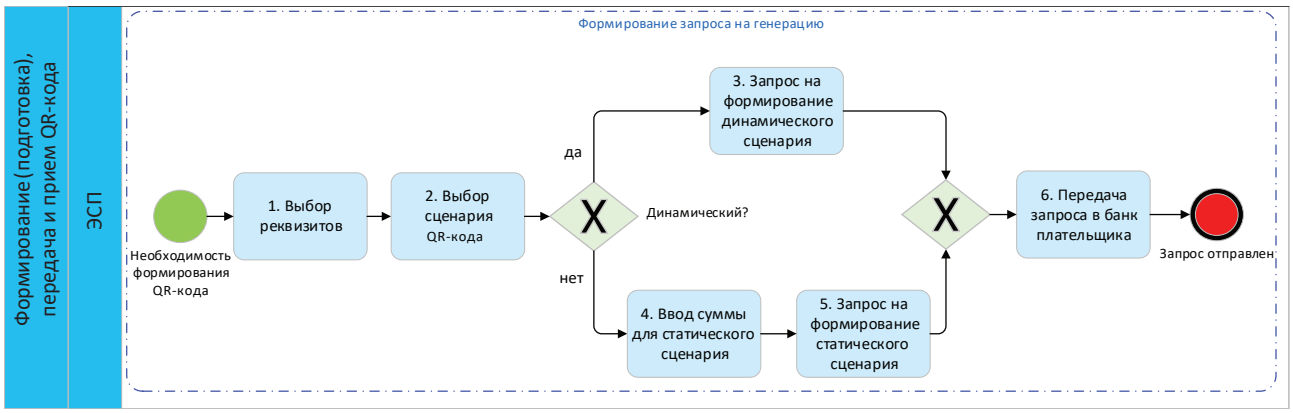
ОПИСАНИЕ СХЕМЫ С ФОРМИРОВАНИЕМ QR-КОДА БАНКОМ ПЛАТЕЛЬЩИКА *Табл. 2*

№	Процесс на технологическом подэтапе	Шаг	Описание
1.	Формирование, передача и прием запроса (данных) для генерации QR-кода (ФППЗ)	Формирование запроса на генерацию	Формирование запроса на генерацию. Плательщик выбирает в ЭСП опцию формирования QR-кода для осуществления перевода денежных средств
2.		Передача запроса на генерацию QR-кода	Запрос на генерацию QR-кода передается из ЭСП поставщику платежного QR-кода
3.		Получение запроса на генерацию QR-кода	Запрос на генерацию получен поставщиком платежного QR-кода, происходит обработка данных плательщика для формирования строки с данными / со ссылкой для QR-кода
4.		Формирование данных для QR-кода	Поставщик платежного QR-кода формирует строку с данными / со ссылкой для QR-кода, которая составляется из данных плательщика
5.		Передача строки для QR-кода	Поставщик платежного QR-кода передает строку с данными / со ссылкой для QR-кода в ЭСП
6.		Получение строки для отображения QR-кода	ЭСП получает строку с данными / со ссылкой для формирования QR-кода в графическом виде
7.	Формирование и представление QR-кода плательщиком/получателем (ФиП)	Отображение QR-кода	ЭСП отображает полученную строку с данными / со ссылкой в виде QR-кода
8.		Представление QR-кода получателю	Плательщик представляет получателю графический QR-код для сканирования
9.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств (СиП)	Сканирование QR-кода	Получатель с помощью устройства сканирования считывает QR-код плательщика, данные которого передаются в приложение получателя
10.		Преобразование QR-кода	Приложение получателя преобразует QR-код плательщика в данные / в ссылку
11.		Передача запроса в банк получателя	Приложение получателя направляет авторизационный запрос с данными / со ссылкой из QR-кода плательщика в банк получателя
12.	Формирование (подготовка), передача и прием электронных сообщений	Передача запроса поставщику платежного QR-кода	Банк получателя передает запрос через платежную систему поставщику платежного QR-кода, который является банком плательщика, чтобы проверить возможность списания денежных средств. При положительном результате проверок денежные средства переводятся стандартным способом

Схема свернутого процесса «Формирование запроса на генерацию» представлена на рис. 3.

Описание схемы шага «Формирование запроса на генерацию» при формировании QR-кода плательщиком в платежном приложении в статическом/динамическом сценарии для осуществления перевода денежных средств представлено в табл. 3.

ПОДПРОЦЕСС «ФОРМИРОВАНИЕ ЗАПРОСА НА ГЕНЕРАЦИЮ» *Рис. 3*



ОПИСАНИЕ СХЕМЫ ПОДПРОЦЕССА «ФОРМИРОВАНИЕ ЗАПРОСА НА ГЕНЕРАЦИЮ» *Табл. 3*

№	Подпроцесс	Шаг	Описание шагов подпроцесса
1.	Формирование запроса на генерацию	Выбор реквизитов	Авторизованный в ЭСП плательщик выбирает реквизиты для формирования QR-кода (если реквизиты для формирования платежного QR-кода не выбраны «по умолчанию»). Далее – шаг 2
2.		Выбор сценария QR-кода	Плательщик выбирает сценарий QR-кода – статический/динамический. При выборе статического сценария QR-кода плательщику необходимо ввести сумму, на которую код будет сформирован. Далее – шаг 4. При выборе динамического сценария QR-кода плательщик не вводит сумму, которая необходима для списания денежных средств. Для использования QR-кода в динамическом сценарии плательщику необходимо находиться в ЭСП в режиме онлайн. Далее – шаг 3. Для статического QR-кода при его формировании рекомендуется уменьшать сумму денежных средств, доступных плательщику для осуществления перевода
3.		Запрос на формирование динамического сценария	Если выбран динамический сценарий для QR-кода, ЭСП передает запрос на его формирование. Далее – шаг 6
4.		Ввод суммы для статического сценария	Если выбран статический сценарий для QR-кода, плательщик в ЭСП вводит сумму, на которую необходимо сформировать данный QR-код. Далее – шаг 5
5.		Запрос на формирование статического сценария	Из ЭСП передается запрос на создание QR-кода в статическом сценарии. Далее – шаг 6
6.		Передача запроса в банк плательщика	Из ЭСП передается запрос на формирование QR-кода в банк плательщика. Далее – шаг 2 основного процесса (рис. 2)

1.2. Поставщик платежного QR-кода – поставщик платежного приложения

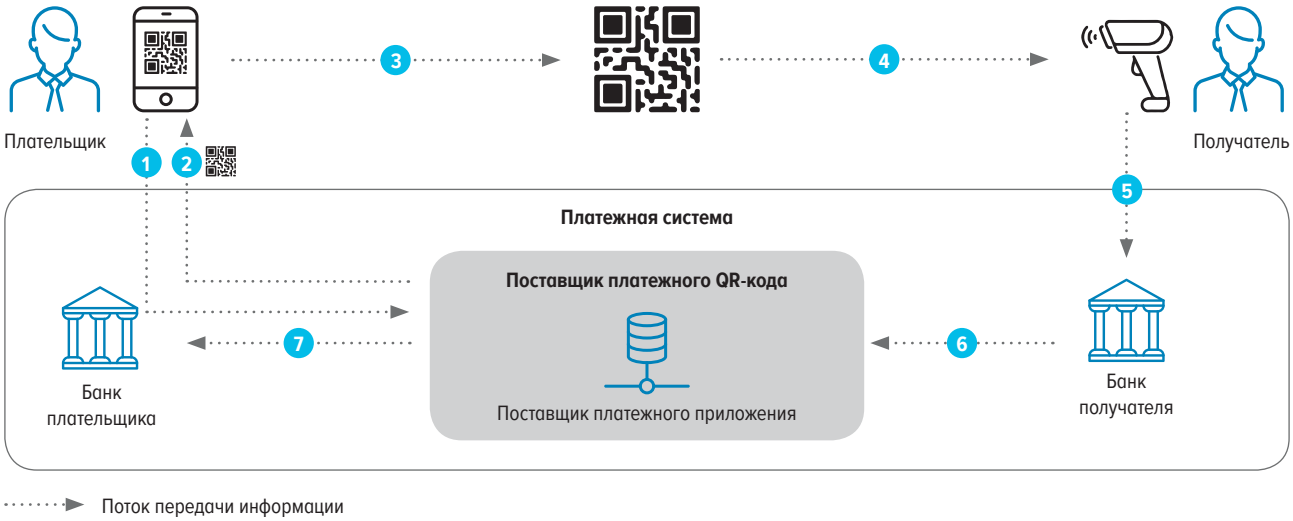
Параметры QR-кода:

- Вид – QR-код плательщика.
- Тип – QR-код с данными / QR-код со ссылкой.
- Сценарии формирования QR-кода:
  - статический для QR-кода с данными;
  - статический для QR-кода со ссылкой;
  - динамический для QR-кода с данными;
  - динамический для QR-кода со ссылкой.

Базовые шаги процесса осуществления переводов денежных средств со сканированием QR-кода с данными / со ссылкой в статическом/динамическом сценариях, представленного на устройстве плательщика, показаны на рис. 4.

Плательщик на устройстве формирует и передает запрос поставщику платежного QR-кода для формирования статического/динамического QR-кода. Поставщик платежного QR-кода возвращает на устройство плательщика строку с данными / со ссылкой для преобразования в графический QR-код. Плательщик представляет получателю QR-код. Получатель сканирует QR-код и передает авторизационный запрос с данными / со ссылкой из QR-кода в банк получателя. Банк получателя передает авторизационный запрос поставщику платежного приложения, где проходит проверка достоверности QR-кода. Если QR-код достоверный, запрос передается в банк плательщика. Далее денежные средства переводятся стандартным способом.

ШАГИ ПРОЦЕССА ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ГЕНЕРАЦИИ QR-КОДА ПОСТАВЩИКОМ ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ *Рис. 4*



ПРОЦЕССЫ ПОДЭТАПА «ФОРМИРОВАНИЕ (ПОДГОТОВКА), ПЕРЕДАЧА И ПРИЕМ QR-КОДА» ПРИ ФОРМИРОВАНИИ QR-КОДА ПОСТАВЩИКОМ ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ *Рис. 5*

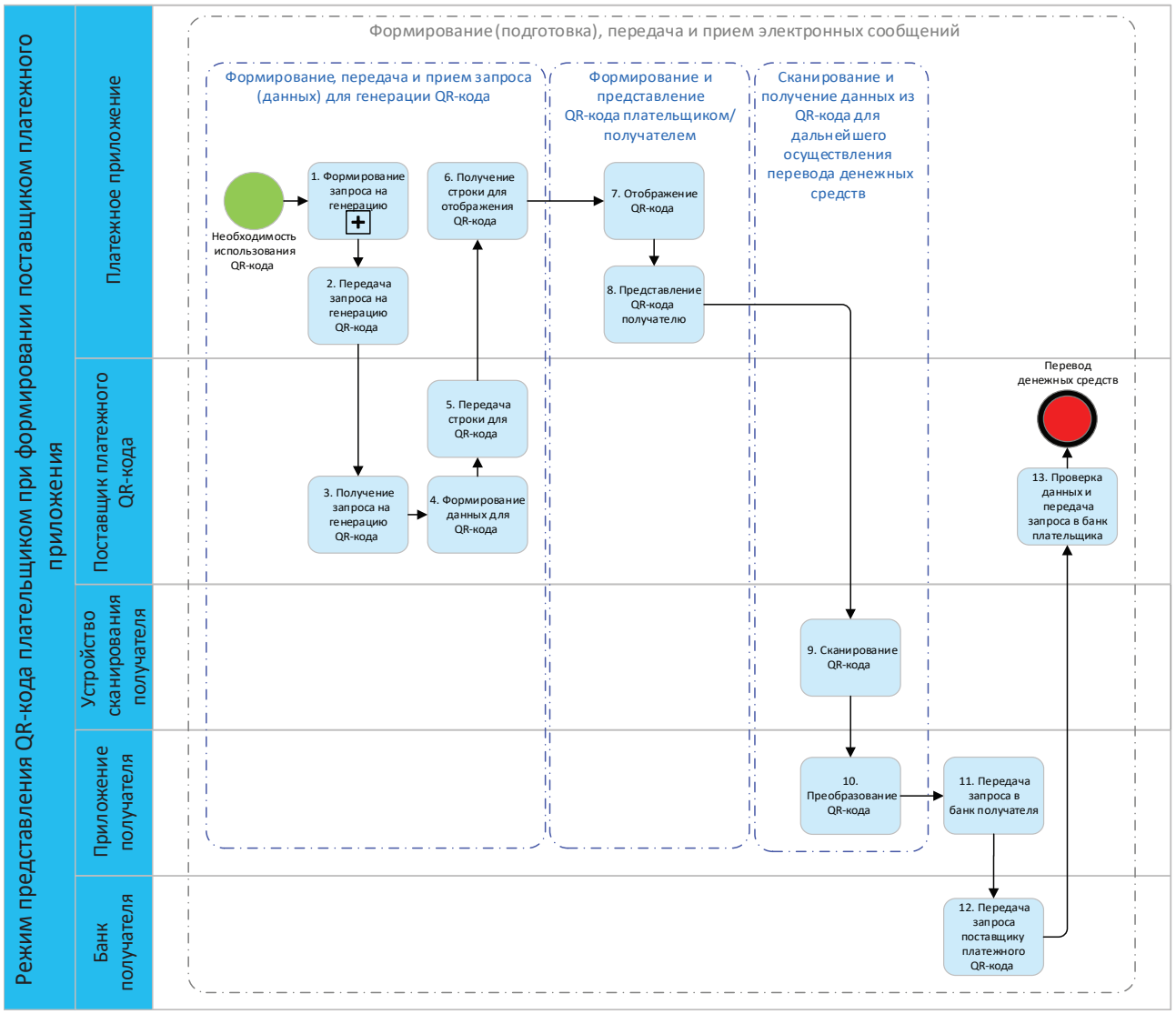


Схема процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода поставщиком платежного приложения представлена на рис. 5.

Описание схемы процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода поставщиком платежного приложения для осуществления переводов денежных средств с представлением QR-кода плательщиком отражено в табл. 4.

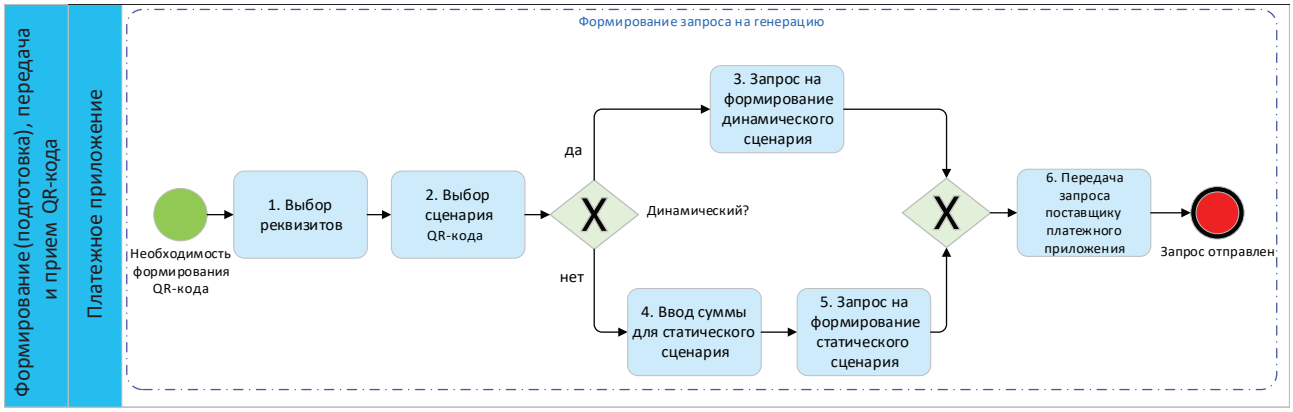
Дополнительные схемы с использованием QR-кода плательщика при формировании поставщиком платежного приложения для сканирования получателем с использованием сканера приведены в приложениях 6, 7 к настоящему стандарту.

ОПИСАНИЕ СХЕМЫ ФОРМИРОВАНИЯ QR-КОДА ПОСТАВЩИКОМ ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ *Табл. 4*

№	Процесс на технологическом подэтапе	Шаг	Описание
1.	Формирование, передача и прием запроса (данных) для генерации QR-кода (ФППЗ)	Формирование запроса на генерацию	Плательщик выбирает в платежном приложении опцию формирования QR-кода для осуществления перевода денежных средств
2.		Передача запроса на генерацию QR-кода	Запрос на генерацию QR-кода передается из платежного приложения поставщику платежного QR-кода
3.		Получение запроса на генерацию QR-кода	Запрос на генерацию получен поставщиком платежного QR-кода, происходит обработка данных плательщика для формирования строки с данными / со ссылкой для QR-кода
4.		Формирование данных для QR-кода	Поставщик платежного QR-кода формирует строку с данными / со ссылкой для QR-кода, которая составляется из данных плательщика
5.		Передача строки для QR-кода	Поставщик платежного QR-кода передает строку с данными / со ссылкой для QR-кода в платежное приложение
6.		Получение строки для отображения QR-кода	Платежное приложение получает строку с данными / со ссылкой для формирования QR-кода в графическом виде
7.	Формирование и представление QR-кода плательщиком/получателем (ФиП)	Отображение QR-кода	Платежное приложение отображает полученную строку с данными / со ссылкой в виде QR-кода
8.		Представление QR-кода получателю	Плательщик представляет получателю графический QR-код для сканирования
9.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств (СиП)	Сканирование QR-кода	Получатель с помощью устройства сканирования считывает QR-код плательщика, данные которого передаются в приложение получателя
10.		Преобразование QR-кода	Приложение получателя преобразует QR-код плательщика в данные / в ссылку
11.	Формирование (подготовка), передача и прием электронных сообщений	Передача запроса в банк получателя	Приложение получателя направляет авторизационный запрос с данными / со ссылкой из QR-кода плательщика в банк получателя
12.		Передача запроса поставщику платежного QR-кода	Банк получателя передает запрос через платежную систему поставщику платежного QR-кода. Поставщик проверяет достоверность данных и при положительном результате передает запрос в банк плательщика
13.		Проверка данных и передача запроса в банк плательщика	Банк плательщика проверяет возможность списания денежных средств, и при положительном результате денежные средства переводятся стандартным способом

Схема свернутого процесса «Формирование запроса на генерацию» представлена на рис. 6.

ПОДПРОЦЕСС «ФОРМИРОВАНИЕ ЗАПРОСА НА ГЕНЕРАЦИЮ» *Рис. 6*



Описание схемы подпроцесса «Формирование запроса на генерацию» при формировании QR-кода плательщиком в платежном приложении в статическом/динамическом сценарии для осуществления перевода денежных средств представлено в табл. 5.

ОПИСАНИЕ СХЕМЫ ПОДПРОЦЕССА «ФОРМИРОВАНИЕ ЗАПРОСА НА ГЕНЕРАЦИЮ» *Табл. 5*

№	Подпроцесс	Шаг	Описание шагов подпроцесса
1.	Формирование запроса на генерацию	Выбор реквизитов	Авторизованный в платежном приложении плательщик выбирает реквизиты, которые будут использоваться для формирования QR-кода (если реквизиты для формирования платежного QR-кода не выбраны «по умолчанию»). Далее – шаг 2
2.		Выбор сценария QR-кода	Плательщик выбирает сценарий QR-кода – статический/динамический. При выборе статического сценария QR-кода плательщику необходимо ввести сумму, на которую он будет сформирован. При выборе динамического сценария QR-кода плательщик не вводит сумму, которая необходима для списания денежных средств. Для использования QR-кода в динамическом сценарии плательщику необходимо находиться в платежном приложении в режиме онлайн. Далее – шаг 3. Для статического QR-кода при его формировании рекомендуется уменьшать сумму денежных средств, доступных плательщику для осуществления перевода
3.		Запрос на формирование динамического сценария	Если выбран динамический сценарий для QR-кода, платежное приложение передает запрос на его формирование. Далее – шаг 6
4.		Ввод суммы для статического сценария	Если выбран статический сценарий для QR-кода, плательщик в платежном приложении вводит сумму, на которую необходимо сформировать данный QR-код. Далее – шаг 5
5.		Запрос на формирование статического сценария	Платежное приложение передает запрос на создание QR-кода в статическом сценарии. Далее – шаг 6
6.		Передача запроса поставщику платежного приложения	Платежное приложение передает запрос на формирование QR-кода поставщику платежного QR-кода. Далее – шаг 2 основного процесса (рис. 5)

2. Режим отображения получателем при формировании поставщиком платежного QR-кода

2.1. Поставщик платежного QR-кода – банк получателя

Параметры QR-кода:

- Вид – QR-код получателя.
- Тип – QR-код с данными / QR-код со ссылкой.
- Сценарии формирования QR-кода:
  - статический для QR-кода с данными;
  - статический для QR-кода со ссылкой;
  - динамический для QR-кода с данными;
  - динамический для QR-кода со ссылкой.

Базовые шаги процесса осуществления переводов денежных средств со сканированием QR-кода с данными в статическом/динамическом сценариях, представленного получателем, показаны на рис. 7.

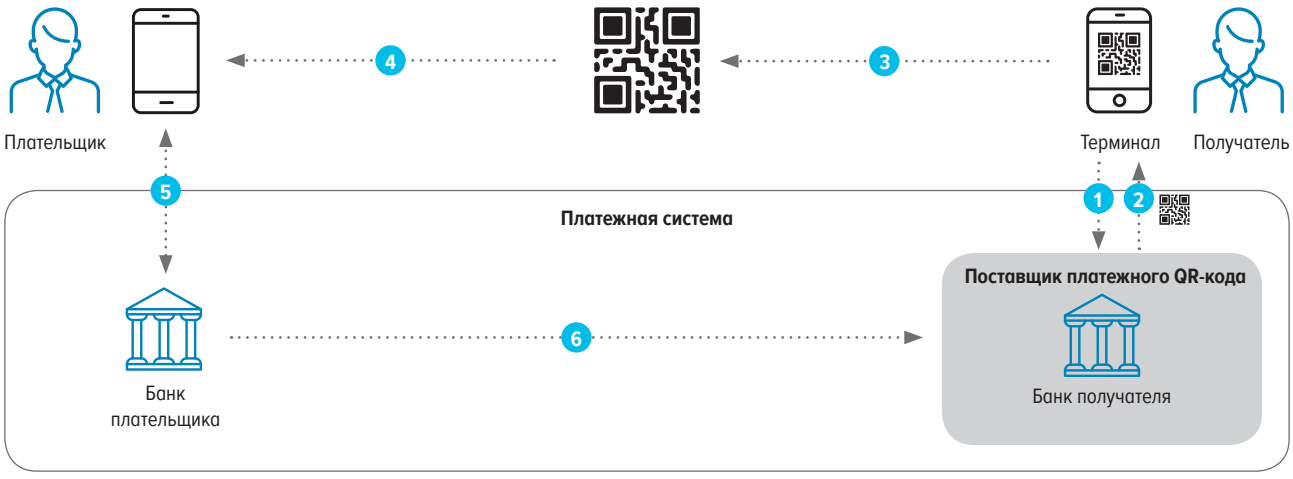
Получатель в приложении формирует и передает запрос поставщику платежного QR-кода для формирования статического/динамического QR-кода. Поставщик платежного QR-кода возвращает в приложение получателя строку с данными / со ссылкой для преобразования в графический QR-код. Получатель предоставляет QR-код плательщику. Плательщик сканирует QR-код и передает запрос на перевод денежных средств в банк плательщика. В случае возможности списания денежные средства переводятся стандартным способом.

Схема процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода банком получателя представлена на рис. 8.

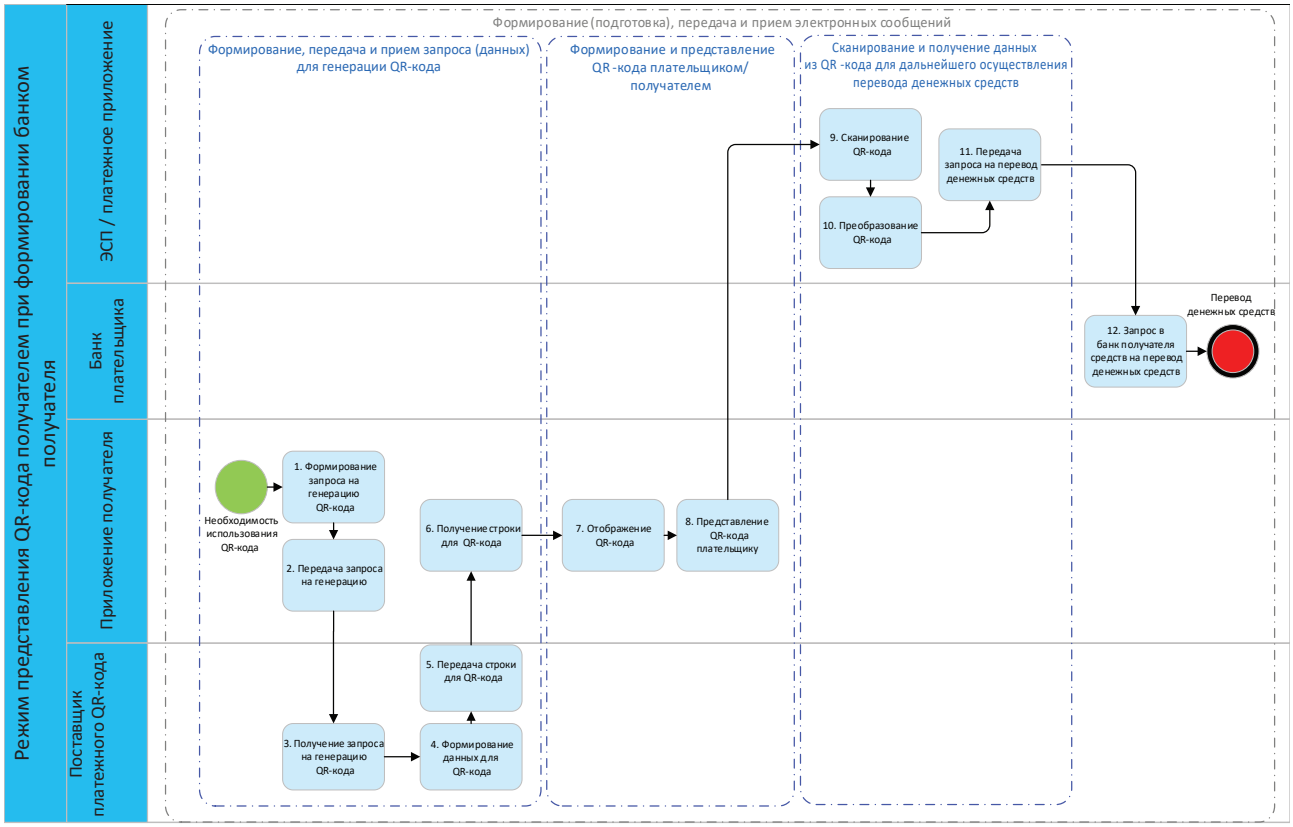
Описание схемы процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода банком получателя для осуществления переводов денежных средств с представлением QR-кода получателем представлено в табл. 6.

Дополнительные схемы с использованием QR-кода получателя при формировании банком получателя для сканирования плательщиком с помощью мобильного устройства приведены в приложениях 8–12 к настоящему стандарту.

ШАГИ ПРОЦЕССА ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ФОРМИРОВАНИИ QR-КОДА БАНКОМ ПОЛУЧАТЕЛЯ *Рис. 7*



ПРОЦЕССЫ ПОДЭТАПА «ФОРМИРОВАНИЕ (ПОДГОТОВКА), ПЕРЕДАЧА И ПРИЕМ QR-КОДА» ПРИ ФОРМИРОВАНИИ QR-КОДА БАНКОМ ПОЛУЧАТЕЛЯ *Рис. 8*



Частная схема с использованием QR-кода получателя при формировании банком получателя, который совпадает с банком плательщика, для сканирования QR-кода в банкомате пользователем с помощью мобильного устройства приведена в приложении 13 к настоящему стандарту.

ОПИСАНИЕ СХЕМЫ С ФОРМИРОВАНИЕМ QR-КОДА БАНКОМ ПОЛУЧАТЕЛЯ *Табл. 6*

№	Процесс на технологическом участке	Шаг	Описание
1.	Формирование, передача и прием запроса (данных) для генерации QR-кода (ФППЗ)	Формирование запроса на генерацию QR-кода	Получатель в своем приложении выбирает опцию формирования QR-кода для оплаты
2.		Передача запроса на генерацию QR-кода	Запрос на генерацию QR-кода вместе с данными платежа передается из приложения получателя поставщику платежного QR-кода
3.		Получение запроса на генерацию QR-кода	Запрос на генерацию получен поставщиком платежного QR-кода
4.		Формирование данных для QR-кода	Поставщик платежного QR-кода формирует строку с данными / со ссылкой для QR-кода, которые составляются из данных получателя и информации о платеже
5.		Передача строки для QR-кода	Поставщик платежного QR-кода передает строку с данными / со ссылкой для QR-кода в приложение получателя
6.		Получение строки для QR-кода	Приложение получателя получило строку с данными / со ссылкой для преобразования в графический QR-код
7.	Формирование и представление QR-кода плательщиком/получателем (ФиП)	Отображение QR-кода	Приложение получателя из полученной строки с данными / со ссылкой формирует графический QR-код
8.		Представление QR-кода плательщику	Получатель предъявляет плательщику QR-код для сканирования

№	Процесс на технологическом участке	Шаг	Описание
9.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств (СиП)	Сканирование QR-кода	Плательщик с использованием камеры на устройстве считывает QR-код, представленный получателем
10.		Преобразование QR-кода	ЭСП / платежное приложение плательщика преобразует QR-код в строку с данными / со ссылкой
11.		Передача запроса на перевод денежных средств	ЭСП / платежное приложение плательщика формирует запрос с данными / со ссылкой из QR-кода на перевод денежных средств и передает его в банк плательщика
12.	Формирование (подготовка), передача и прием электронного сообщения	Запрос в банк получателя средств на перевод денежных средств	Банк плательщика формирует запрос на перевод денежных средств и передает его через платежную систему в банк получателя. Банк получателя проверяет возможность зачисления денежных средств получателю и передает ответ через платежную систему в банк плательщика. Банк плательщика переводит денежные средства плательщика для зачисления получателю

2.2. Поставщик платежного QR-кода – сторонняя организация, формирующая QR-код в прикладном ПО

Параметры QR-кода:

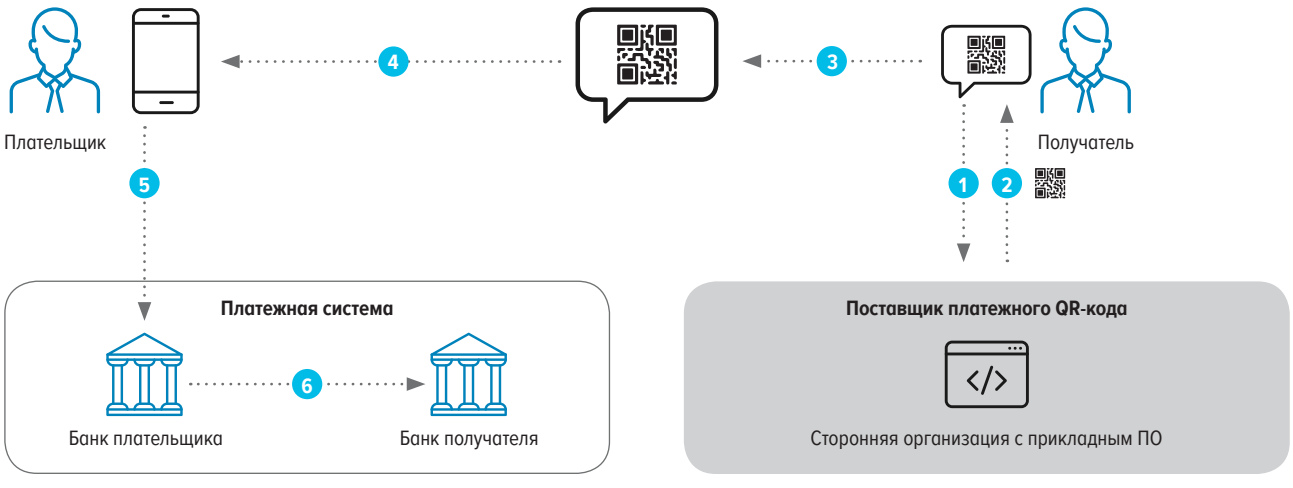
- Вид – QR-код получателя.
- Тип – QR-код с данными.
- Сценарий формирования QR-кода – статический.

Базовые шаги процесса осуществления переводов денежных средств со сканированием QR-кода с данными в статическом сценарии, представленного получателем в квитанции, показаны на рис. 9.

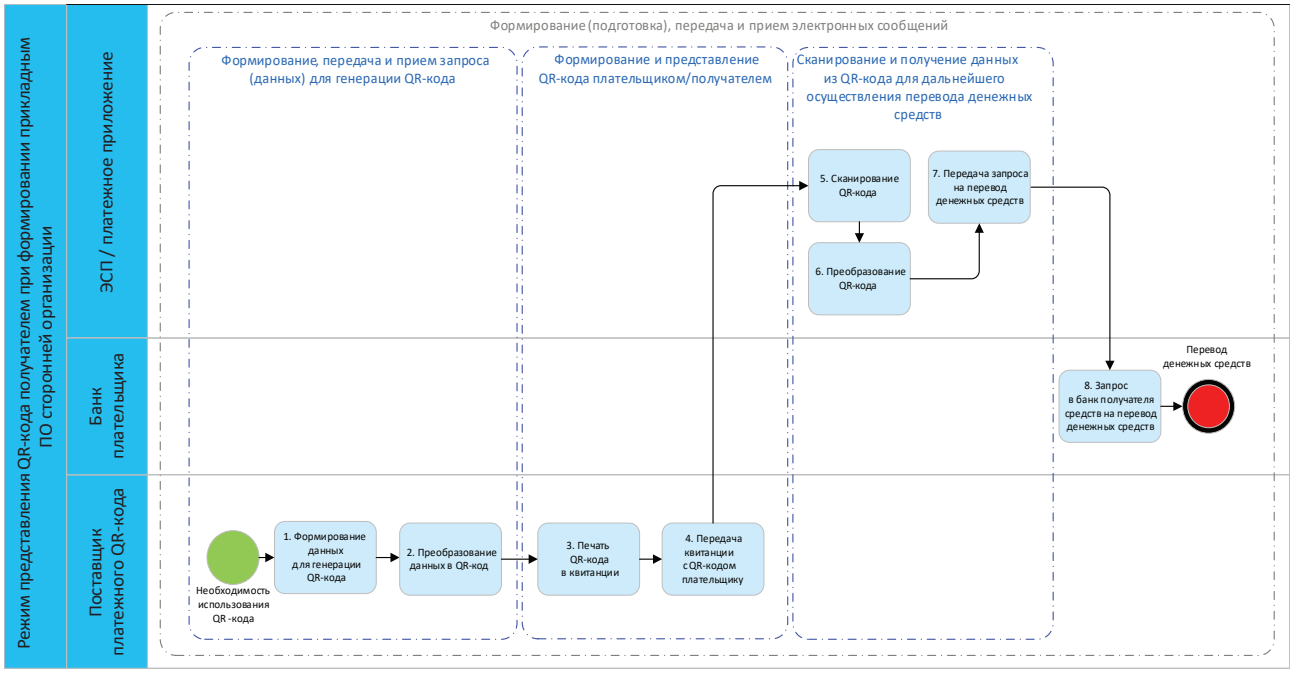
Получатель в приложении организации заполняет свои реквизиты, которые будут использоваться плательщиком для последующего осуществления перевода денежных средств. Получатель в приложении организации формирует QR-код в статическом сценарии и печатает его в квитанции для последующей оплаты плательщиком. Плательщик в полученной квитанции сканирует QR-код с использованием мобильного устройства, реквизиты операции автоматически заполняются в ЭСП / платежном приложении, и далее денежные средства переводятся стандартным способом.

Схема процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода сторонней организацией с использованием прикладного ПО организации представлена на рис. 10.

ШАГИ ПРОЦЕССА ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ФОРМИРОВАНИИ QR-КОДА СТОРОННЕЙ ОРГАНИЗАЦИЕЙ *Рис. 9*



ПРОЦЕССЫ ПОДЭТАПА «ФОРМИРОВАНИЕ (ПОДГОТОВКА), ПЕРЕДАЧА И ПРИЕМ QR-КОДА» ПРИ ФОРМИРОВАНИИ QR-КОДА СТОРОННЕЙ ОРГАНИЗАЦИЕЙ *Рис. 10*



Описание схемы процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода в прикладном ПО сторонней организации для осуществления переводов денежных средств с представлением QR-кода получателем в квитанции отражено в табл. 7.

Дополнительная схема с использованием QR-кода получателя при формировании в прикладном ПО сторонней организации для сканирования плательщиком с помощью мобильного устройства приведена в приложении 14 к настоящему стандарту.

ОПИСАНИЕ СХЕМЫ С ФОРМИРОВАНИЕМ QR-КОДА В ПРИКЛАДНОМ ПО СТОРОННЕЙ ОРГАНИЗАЦИИ *Табл. 7*

№	Процесс на технологическом участке	Шаг	Описание
1.	Формирование, передача и прием запроса (данных) для генерации QR-кода (ФППЗ)	Формирование данных для генерации QR-кода	Поставщик платежного QR-кода формирует данные, необходимые для осуществления перевода денежных средств плательщиком
2.		Преобразование данных в QR-код	Поставщик платежного QR-кода преобразует данные получателя в QR-код
3.	Формирование и представление QR-кода плательщиком/получателем (ФиП)	Печать QR-кода в квитанции	Поставщик платежного QR-кода печатает QR-код в квитанции
4.		Передача квитанции с QR-кодом плательщику	Квитанция с QR-кодом отправлена плательщику для осуществления перевода денежных средств
5.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств (СиП)	Сканирование QR-кода	Плательщик в ЭСП / платежном приложении сканирует QR-код из квитанции
6.		Преобразование QR-кода	ЭСП / платежное приложение плательщика преобразует QR-код в данные
7.		Передача запроса на перевод денежных средств	ЭСП / платежное приложение плательщика формирует запрос с данными из QR-кода на перевод денежных средств и передает его в банк плательщика
8.	Формирование (подготовка), передача и прием электронного сообщения	Запрос в банк получателя средств на перевод денежных средств	Банк плательщика проверяет возможность списания денежных средств. При положительном результате передается запрос в банк получателя на перевод денежных средств

2.3. Поставщик платежного QR-кода – ОПКЦ СБП

Параметры QR-кода:

- Вид – QR-код получателя.
- Тип – QR-код со ссылкой.
- Сценарии формирования QR-кода:
  - статический QR-код со ссылкой;
  - динамический QR-код со ссылкой.

Базовые шаги процесса осуществления переводов денежных средств со сканированием QR-кода со ссылкой в статическом/динамическом сценариях, представленного получателем, показаны на рис. 11.

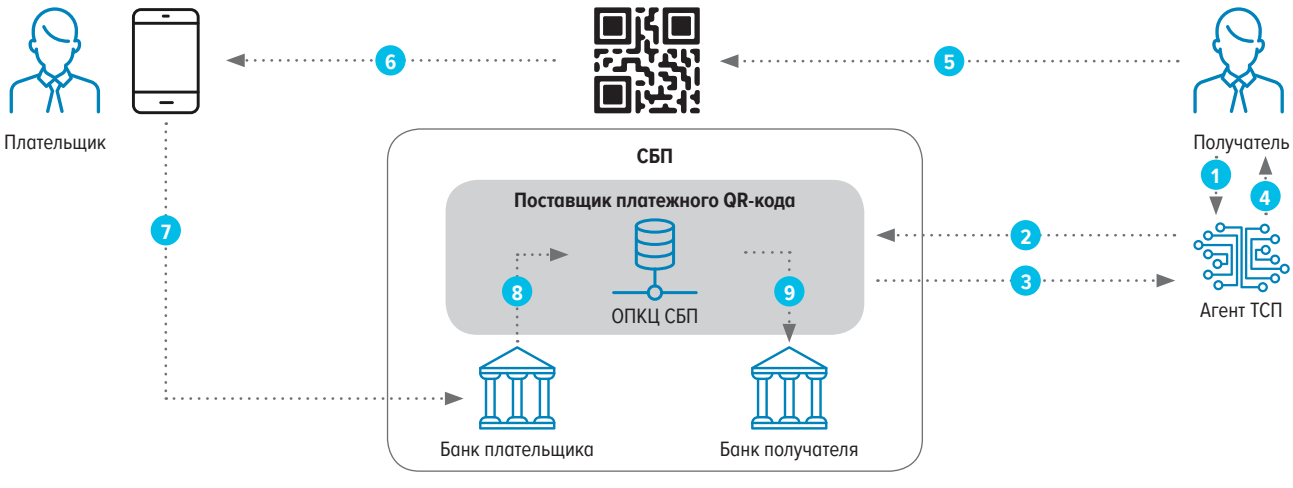
Получатель заполняет реквизиты, необходимые для осуществления перевода денежных средств плательщиком. Получатель передает данные для формирования QR-кода агенту ТСП. Агент ТСП проверяет данные получателя и передает запрос в ОПКЦ СБП. ОПКЦ СБП возвращает строку для QR-кода агенту ТСП. Агент ТСП передает QR-код / строку для QR-кода получателю (в зависимости от способа представления получателем). Плательщик сканирует QR-код получателя с использованием мобильного устройства и передает запрос на перевод денежных средств в банк плательщика. Далее осуществляется стандартная операция СБП С2В, регламентированная стандартами ОПКЦ СБП.

Схема процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода ОПКЦ СБП представлена на рис. 12.

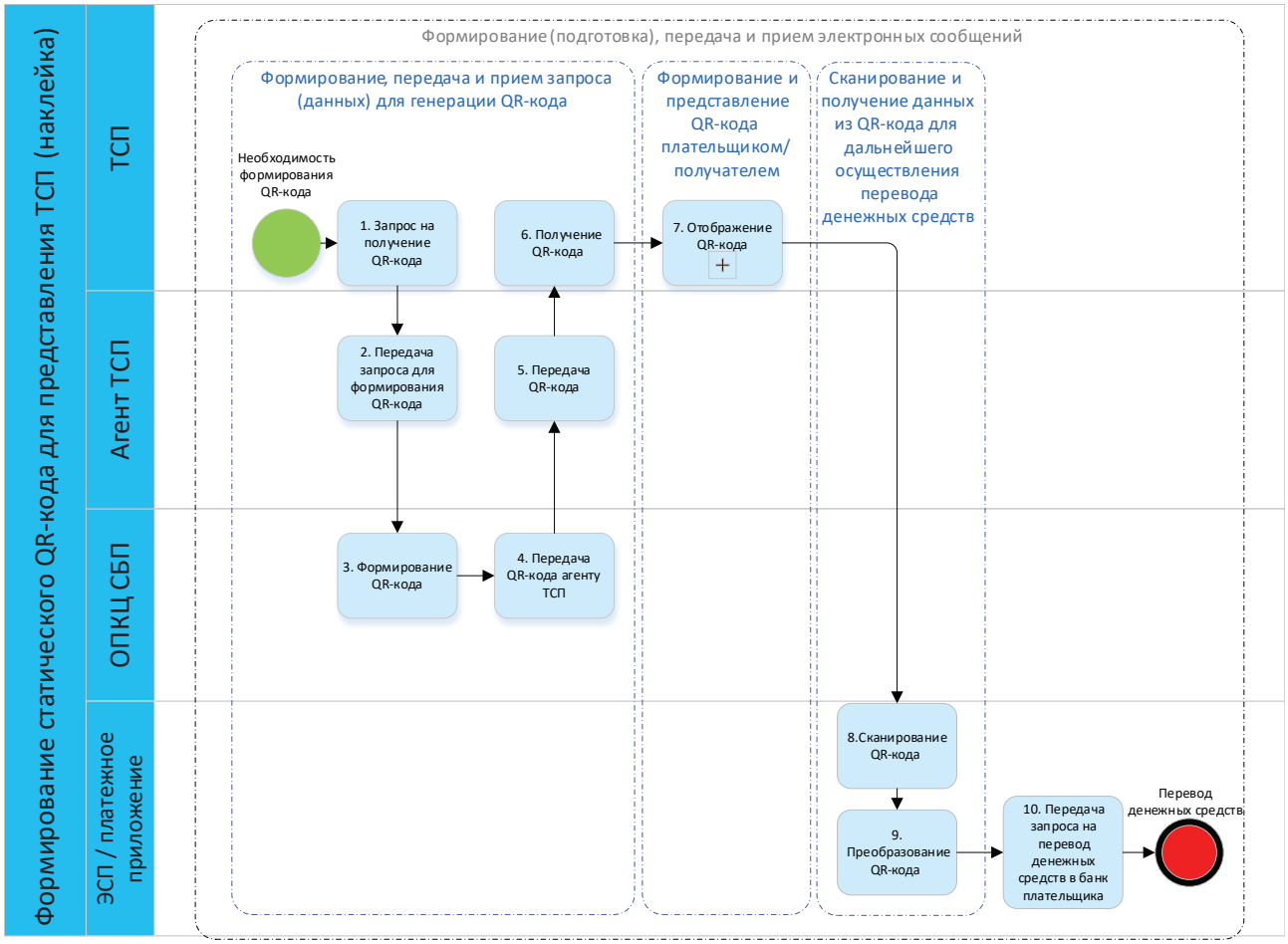
Схема процессов на технологическом подэтапе «Формирование (подготовка), передача и прием QR-кода» при формировании QR-кода ОПКЦ СБП для осуществления переводов денежных средств СБП С2В с представлением QR-кода получателем описана в табл. 8.

Дополнительные схемы с использованием QR-кода получателя при формировании ОПКЦ СБП для сканирования плательщиком с помощью смартфона приведены в приложениях 15–21 к настоящему стандарту.

ШАГИ ПРОЦЕССА ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ФОРМИРОВАНИИ QR-КОДА ОПКЦ СБП *Рис. 11*



ПРОЦЕССЫ ПОДЭТАПА «ФОРМИРОВАНИЕ (ПОДГОТОВКА), ПЕРЕДАЧА И ПРИЕМ QR-КОДА» ПРИ ФОРМИРОВАНИИ QR-КОДА ОПКЦ СБП *Рис. 12*



ОПИСАНИЕ СХЕМЫ С ФОРМИРОВАНИЕМ QR-КОДА ОПКЦ СБП *Табл. 8*

№	Процесс на технологическом участке	Шаг	Описание
1.	Формирование, передача и прием запроса (данных) для генерации QR-кода (ФПП3)	Запрос на получение QR-кода	ТСП формирует и передает запрос с данными для QR-кода
2.		Передача запроса для формирования QR-кода	Агент ТСП получил, проверил запрос с данными от ТСП и отправил его в ОПКЦ СБП
3.		Формирование QR-кода	ОПКЦ СБП получил запрос от агента ТСП, сформировал строку для QR-кода
4.		Передача QR-кода агенту ТСП	ОПКЦ СБП передает строку для QR-кода агенту ТСП
5.		Передача QR-кода	Агент ТСП передает строку для QR-кода / QR-код в ТСП (в зависимости от сценария передается строка или QR-код)
6.		Получение QR-кода	ТСП получил QR-код
7.	Формирование и представление QR-кода плательщиком/получателем (ФиП)	Отображение QR-кода	QR-код представлен плательщику для сканирования
8.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств (СиП)	Сканирование QR-кода	Плательщик в ЭСП / платежном приложении сканирует QR-код
9.		Преобразование QR-кода	QR-код в ЭСП / платежном приложении преобразуется в данные и отображается плательщику, который подтверждает осуществление перевода денежных средств
10.	Формирование (подготовка), передача и прием электронного сообщения	Передача запроса на перевод денежных средств в банк плательщика	Запрос на перевод денежных средств передается из ЭСП / платежного приложения в банк плательщика

ПОДПРОЦЕСС «ОТОБРАЖЕНИЕ QR-КОДА» *Рис. 13*

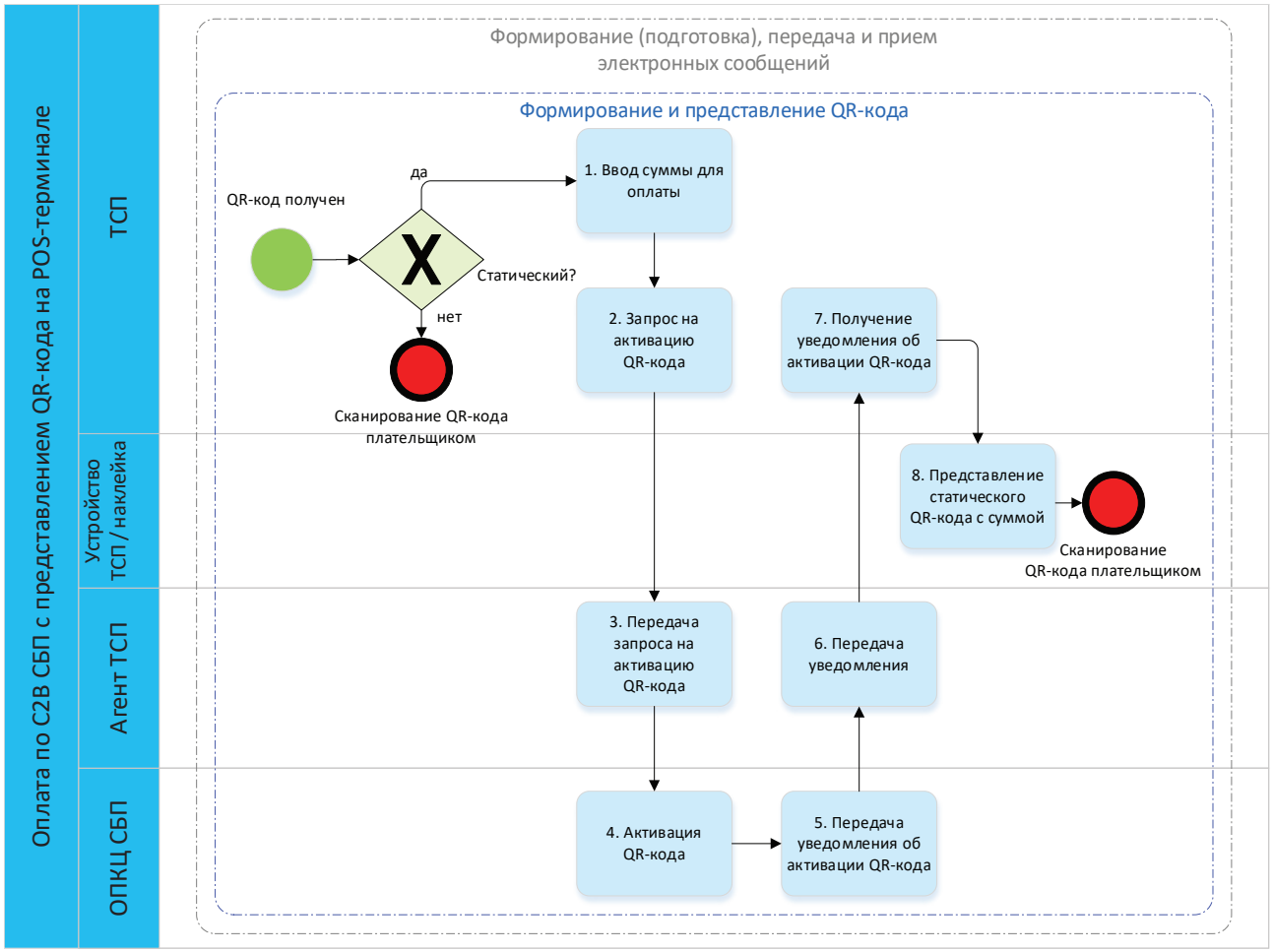


Схема свернутого подпроцесса «Отображение QR-кода» представлена на рис. 13.

Описание схемы с отображением QR-кода, сформированного ОПКЦ СБП, представлено в табл. 9.

ОПИСАНИЕ СХЕМЫ С ОТОБРАЖЕНИЕМ QR-КОДА ОПКЦ СБП *Табл. 9*

№	Процесс на технологическом участке	Шаг	Описание
1.	Формирование и представление QR-кода	Ввод суммы для оплаты	В приложении ТСП вводится сумма для оплаты по статическому QR-коду
2.		Запрос на активацию QR-кода	Из приложения ТСП передается запрос агенту ТСП для активации QR-кода
3.		Передача запроса на активацию QR-кода	Агент ТСП передает запрос на активацию QR-кода в ОПКЦ СБП
4.		Активация QR-кода	ОПКЦ СБП проверяет и активирует QR-код
5.		Передача уведомления об активации QR-кода	ОПКЦ СБП отправил уведомление агенту ТСП об активации QR-кода
6.		Передача уведомления	Агент ТСП отправил уведомление об активации QR-кода в приложение ТСП
7.		Получение уведомления об активации QR-кода	В приложении ТСП получено уведомление об активации QR-кода
8.		Представление статического QR-кода с суммой	QR-код в статическом сценарии с суммой представлен плательщику на устройстве ТСП / наклейке

ПРИЛОЖЕНИЕ 3. ПРИМЕРЫ РЕАЛИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ С ИСПОЛЬЗОВАНИЕМ ТИПОВЫХ СЦЕНАРИЕВ ПРИМЕНЕНИЯ QR-КОДОВ

В табл. 10 представлен перечень типовых сценариев реализации переводов денежных средств с использованием QR-кодов.

СПИСОК СЦЕНАРИЕВ РЕАЛИЗАЦИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ *Табл. 10*

Процессы оплаты по QR-коду					
№	**Процесс оплаты с QR-кодом**	**Представление QR-кода**	**Способ сканирования**	**Сценарий использования**	**Приложение**
1.	Процесс оплаты с представлением статического/динамического QR-кода в ЭСП	ЭСП	Сканер получателя	Статический/ динамический	Приложение 4
2.	Процесс списания/зачисления наличных денежных средств в банкомате с использованием ЭСП	ЭСП	Сканер банкомата	Статический/ динамический	Приложение 5
3.	Процесс оплаты с представлением QR-кода в платежном приложении	Платежное приложение	Сканер получателя	Статический/ динамический	Приложение 6
4.	Процесс списания/зачисления наличных денежных средств в банкомате с использованием платежного приложения	Платежное приложение	Сканер банкомата	Статический/ динамический	Приложение 7
5.	Процесс оплаты с представлением QR-кода на POS-терминале ТСП	Получатель	Камера телефона плательщика	Динамический	Приложение 8
6.	Процесс оплаты с представлением QR-кода на кассе ТСП (экран продавца) – *монитор, планшет, телефон*	Получатель	Камера телефона плательщика	Статический/ динамический	Приложение 9 Приложение 10
7.	Процесс оплаты с представлением QR-кода на физическом носителе в ТСП (наклейка)	Получатель	Камера телефона плательщика	Статический	Приложение 11
8.	Процесс оплаты в финтехприложении по QR-коду	Получатель	Камера телефона плательщика / переход по ссылке на телефоне плательщика	Статический/ динамический	Приложение 12
9.	Процесс списания/зачисления наличных денежных средств	Банкомат	Камера телефона пользователя	Динамический	Приложение 13
10.	Процесс оплаты с представлением QR-кода в квитанции (бумажный носитель)	Получатель	Камера телефона плательщика	Статический	Приложение 14
11.	Процесс оплаты по C2B СБП с представлением QR-кода на кассе ТСП (наклейка)	Получатель	Камера телефона плательщика	Статический	Приложение 15
12.	Процесс оплаты по C2B СБП с представлением на POS-терминале	Получатель	Камера телефона плательщика	Статический/ динамический	Приложение 16 Приложение 17
13.	Процесс оплаты по C2B СБП с представлением на мониторе ТСП / веб-браузере	Получатель	Камера телефона плательщика	Статический/ динамический	Приложение 18 Приложение 19
14.	Процесс оплаты по B2B СБП с представлением на мониторе	Получатель	Камера телефона плательщика	Статический/ динамический	Приложение 20 Приложение 21

ПРИЛОЖЕНИЕ 4. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО/ ДИНАМИЧЕСКОГО QR-КОДА В ЭСП

Сценарий процесса

Плательщик проходит аутентификацию в ЭСП, выбирает реквизиты для оплаты, статический/динамический сценарий для QR-кода (для статического сценария вводится сумма), передает запрос на формирование поставщику платежного QR-кода (банк плательщика).

Поставщик платежного QR-кода проверяет возможность формирования QR-кода. При положительном результате проверок формируется QR-код (для QR-кода в статическом сценарии рекомендовано уменьшать сумму денежных средств, доступных плательщику для осуществления перевода).

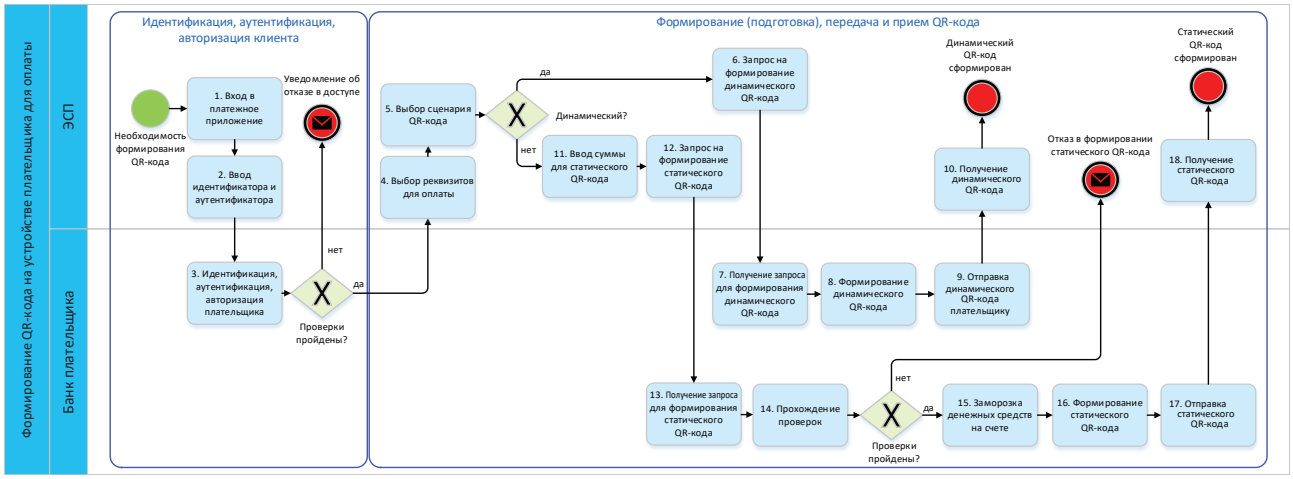
Плательщик представляет QR-код получателю для сканирования. Получатель сканирует QR-код и передает авторизационный запрос в банк получателя. Банк получателя передает запрос в банк плательщика через платежную систему. Банк плательщика проверяет возможность перевода денежных средств. При положительном результате банк плательщика списывает денежные средства плательщика, банк получателя зачисляет денежные средства получателю.

Схемы процесса представлены на рис. 14–16. Меры защиты на технологических участках и подэтапах приведены в табл. 11.

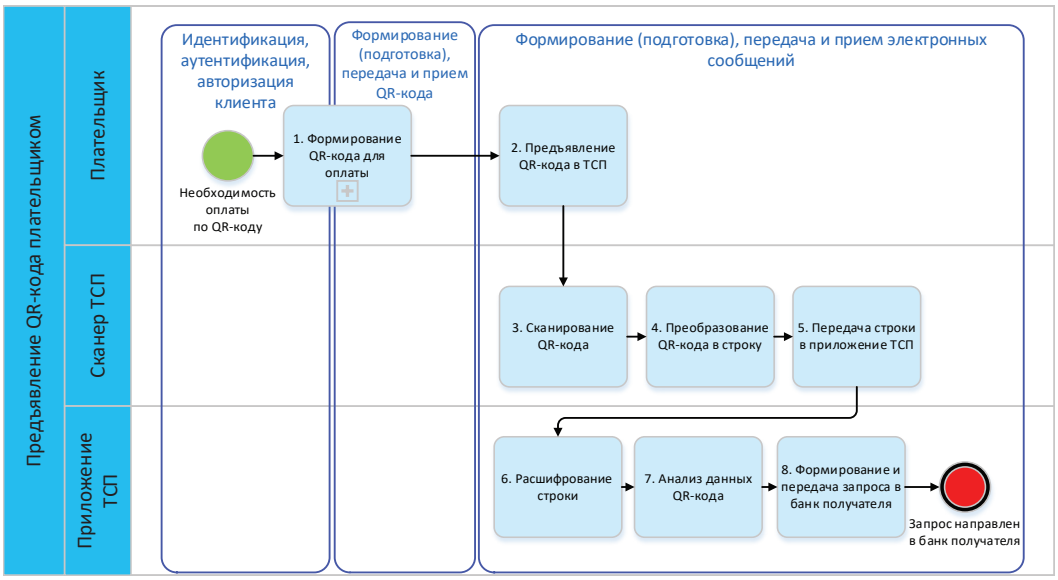
МЕРЫ ЗАЩИТЫ ДЛЯ QR-КОДОВ В ПЛАТЕЖНОМ ПРИЛОЖЕНИИ ПРИ ОСУЩЕСТВЛЕНИИ ОПЛАТЫ *Табл. 11*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.3.2, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	1.1.6, 2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 2.4.2, 3.2.4

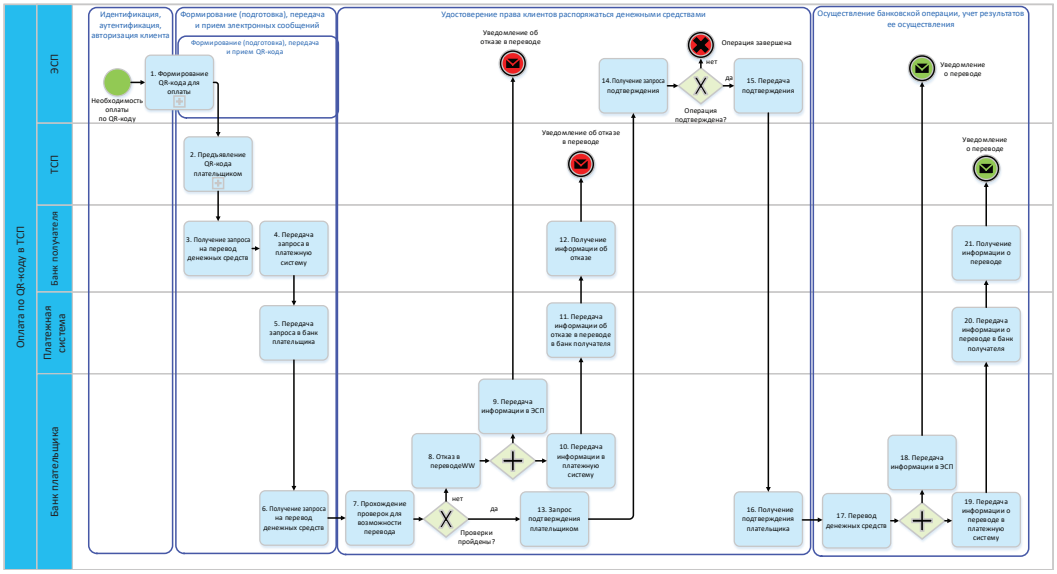
ФОРМИРОВАНИЕ QR-КОДА В ЭСП *Рис. 14*



ПРЕДЪЯВЛЕНИЕ QR-КОДА ПЛАТЕЛЬЩИКОМ *Рис. 15*



ОПЛАТА ПО QR-КОДУ В ТСП *Рис. 16*



ПРИЛОЖЕНИЕ 5. ПРОЦЕСС СНЯТИЯ/ВНЕСЕНИЯ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ С ИСПОЛЬЗОВАНИЕМ ЭСП

Сценарий процесса

Пользователь проходит аутентификацию в ЭСП, выбирает реквизиты для оплаты, статический/динамический сценарий для QR-кода (для статического сценария вводится сумма), передает запрос на формирование поставщику платежного QR-кода (банк плательщика).

Поставщик платежного QR-кода проверяет возможность формирования QR-кода.
При положительном результате проверок формируется QR-код (для QR-кода в статическом сценарии рекомендуется уменьшать сумму денежных средств на счете, доступных плательщику для осуществления перевода).

Пользователь предъявляет QR-код в банкомате для снятия денежных средств. Банкомат сканирует и передает запрос в банк пользователя, чтобы проверить возможность снятия денежных средств. При положительном результате проверок передается запрос в ЭСП плательщика для подтверждения операции и указания суммы денежных средств. После подтверждения банк плательщика проверяет его корректность, уменьшает сумму денежных средств на счете, доступных пользователю для осуществления перевода, и выдает наличные денежные средства пользователю.

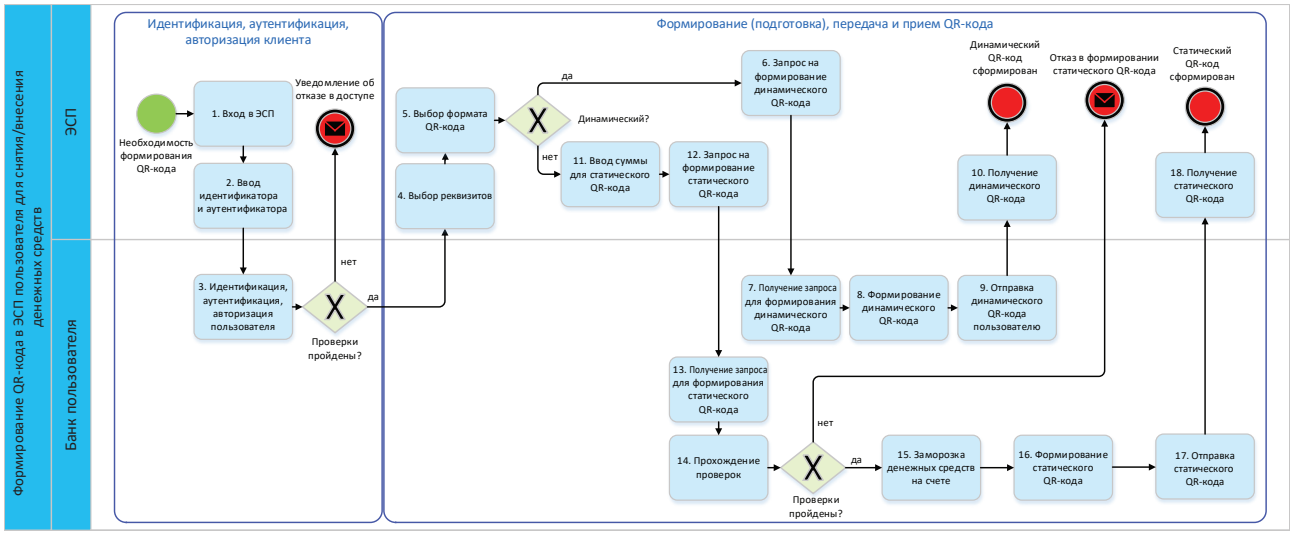
Пользователь предъявляет QR-код в банкомате для внесения денежных средств. Банкомат сканирует и передает запрос в банк пользователя, чтобы проверить возможность внесения денежных средств. При положительном результате проверок передается запрос в ЭСП пользователя для подтверждения операции. После подтверждения банк пользователя проверяет его корректность, передает уведомление в банкомат о возможности внесения денежных средств. Пользователь вносит денежные средства в банкомат, который передает информацию в банк пользователя о необходимости зачисления суммы денежных средств на счет.

Схемы процесса представлены на рис. 17–20. Меры защиты на технологических участках и подэтапах приведены в табл. 12.

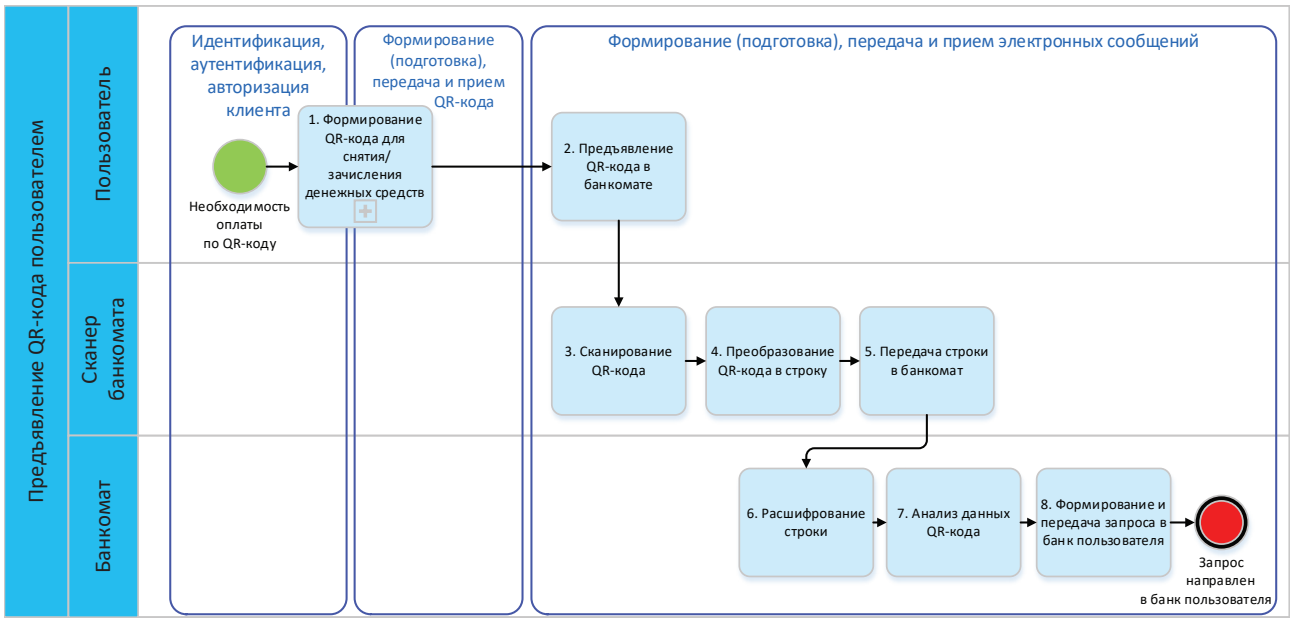
МЕРЫ ЗАЩИТЫ ДЛЯ QR-КОДОВ В ЭСП ПРИ СНЯТИИ/ВНЕСЕНИИ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ *Табл. 12*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 3.2.4

ФОРМИРОВАНИЕ QR-КОДА В ЭСП ДЛЯ СНЯТИЯ/ВНЕСЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ *Рис. 17*

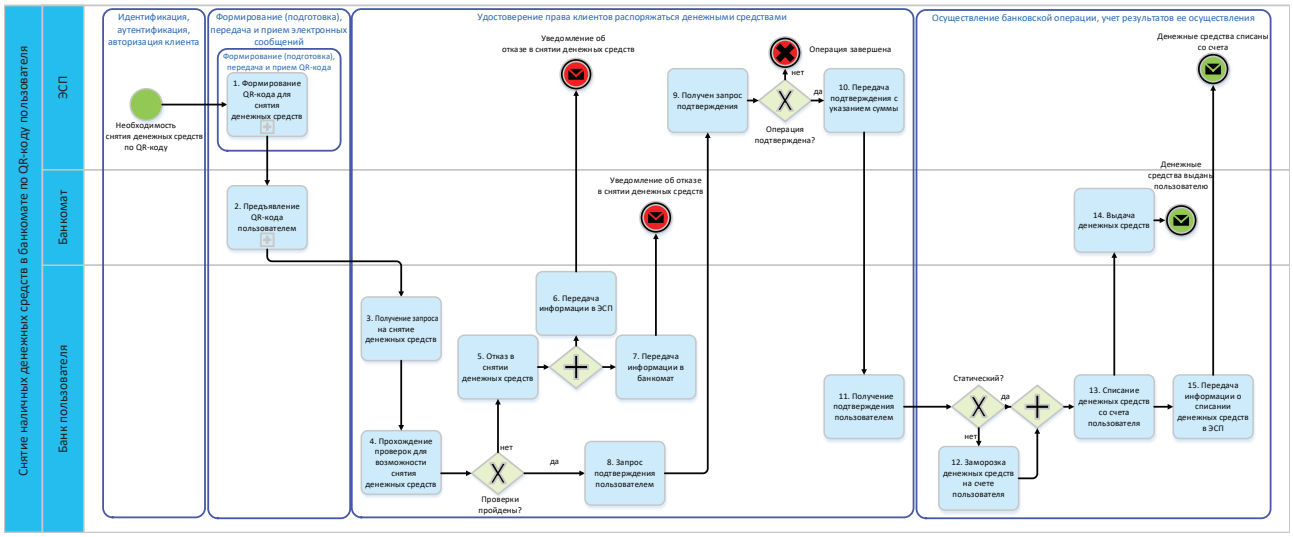


ПРЕДЪЯВЛЕНИЕ QR-КОДА ПОЛЬЗОВАТЕЛЕМ *Рис. 18*



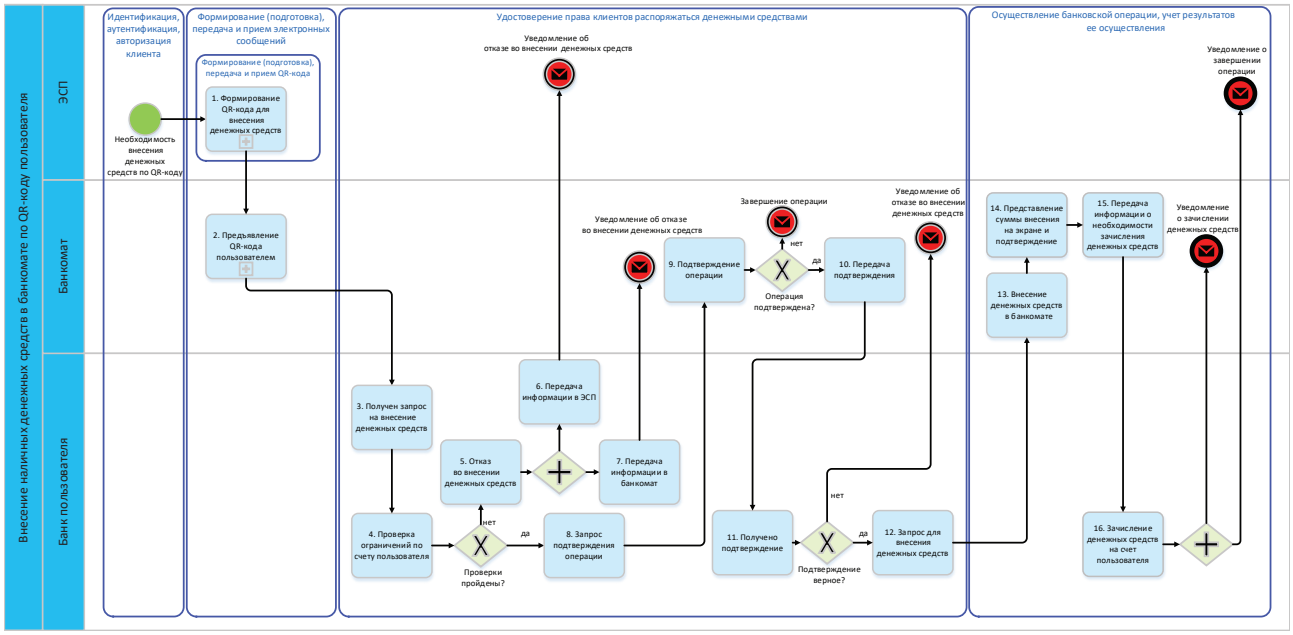
СНЯТИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ ПО QR-КОДУ ПОЛЬЗОВАТЕЛЯ

Рис. 19



ВНЕСЕНИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ ПО QR-КОДУ ПОЛЬЗОВАТЕЛЯ

Рис. 20



ПРИЛОЖЕНИЕ 6. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО/ ДИНАМИЧЕСКОГО QR-КОДА В ПЛАТЕЖНОМ ПРИЛОЖЕНИИ

Сценарий процесса

Плательщик в платежном приложении добавляет токенизированную (цифровую) карту для возможности формирования QR-кода в статическом/динамическом сценарии.

Плательщик выбирает карту, статический/динамический сценарий для формирования QR-кода и передает запрос на его создание (для QR-кода в статическом сценарии вводится сумма). Сервер поставщика платежного приложения передает запрос через платежную систему в сервис токенизации на поиск соответствующего токена. При наличии данных карты по соответствующему токену передается запрос в банк плательщика через платежную систему, чтобы проверить возможность перевода денежных средств. Банк плательщика при положительном результате проверок передает ответ на запрос через платежную систему на сервер поставщика платежного приложения (для QR-кода в статическом сценарии рекомендуется осуществлять заморозку денежных средств на карте плательщика). На сервере поставщика платежного приложения формируется QR-код и передается в платежное приложение.

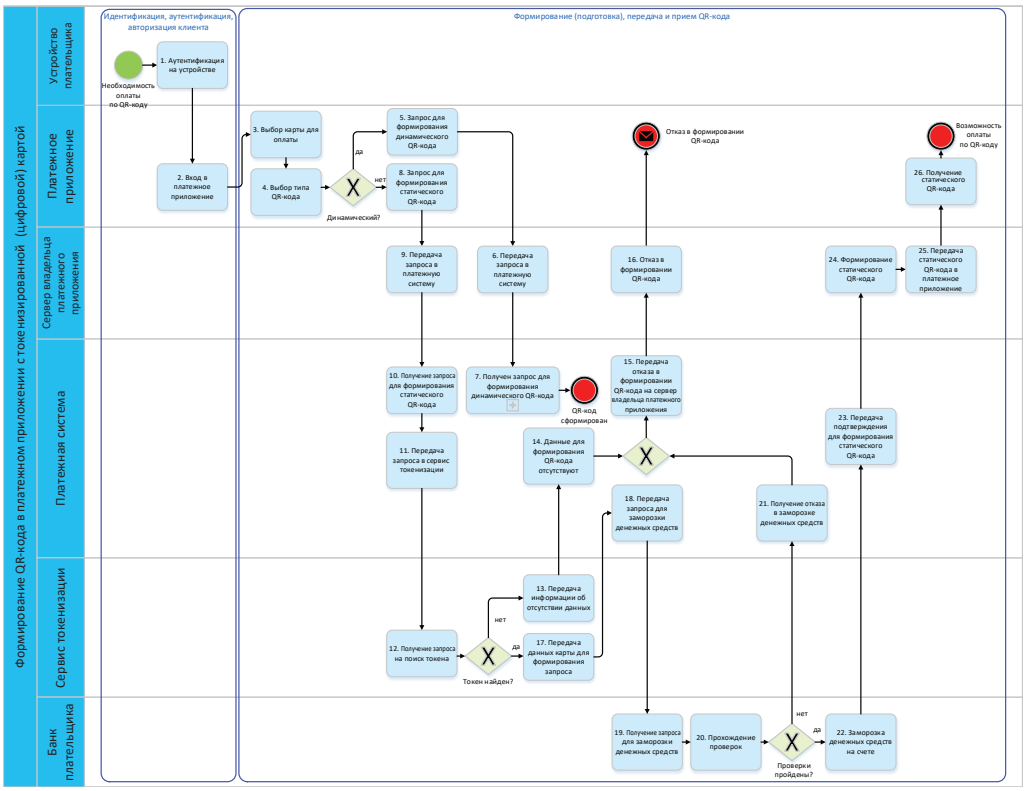
Плательщик представляет получателю QR-код для сканирования. Получатель сканирует QR-код и передает авторизационный запрос в банк получателя. Банк получателя передает авторизационный запрос в платежную систему. Платежная система передает запрос на поиск токена в сервис токенизации. При наличии токена передается запрос с данными из платежной системы в банк плательщика. Банк плательщика проверяет возможность осуществления перевода денежных средств. При положительном результате проверок банк плательщика списывает денежные средства со счета плательщика, банк получателя зачисляет денежные средства на счет получателя.

Схемы процесса представлены на рис. 21–24. Меры защиты на технологических участках и подэтапах приведены в табл. 13.

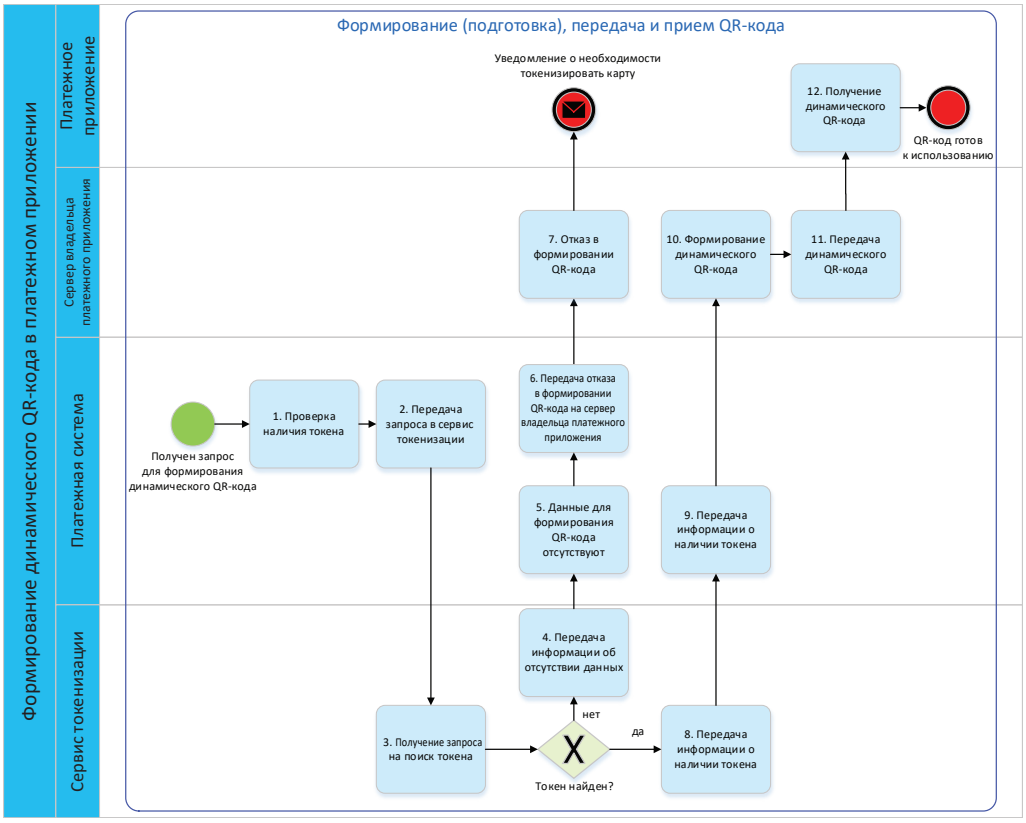
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО СТАТИЧЕСКОМУ/ДИНАМИЧЕСКОМУ QR-КОДУ В ПЛАТЕЖНОМ ПРИЛОЖЕНИИ *Табл. 13*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.2.1, 1.2.2, 1.3.1–1.3.3, 1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.3.2
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3, 3.4.4
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 3.2.4

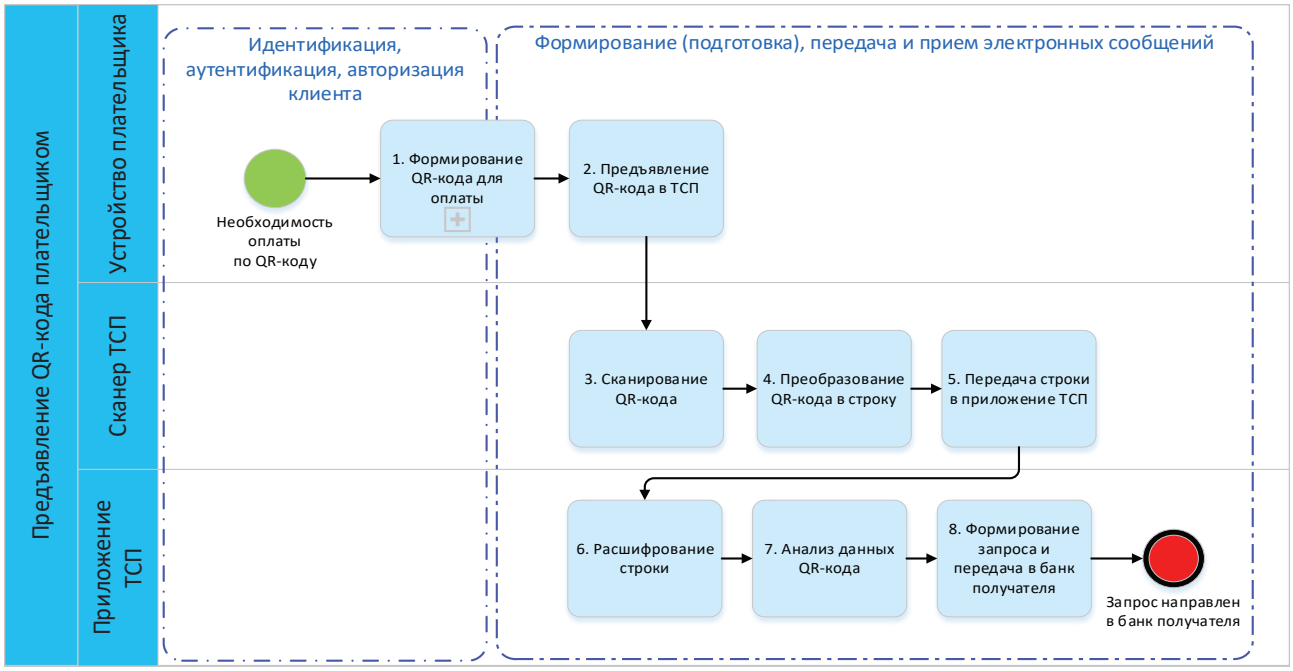
ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА В ПЛАТЕЖНОМ ПРИЛОЖЕНИИ ДЛЯ ОПЛАТЫ *Рис. 21*



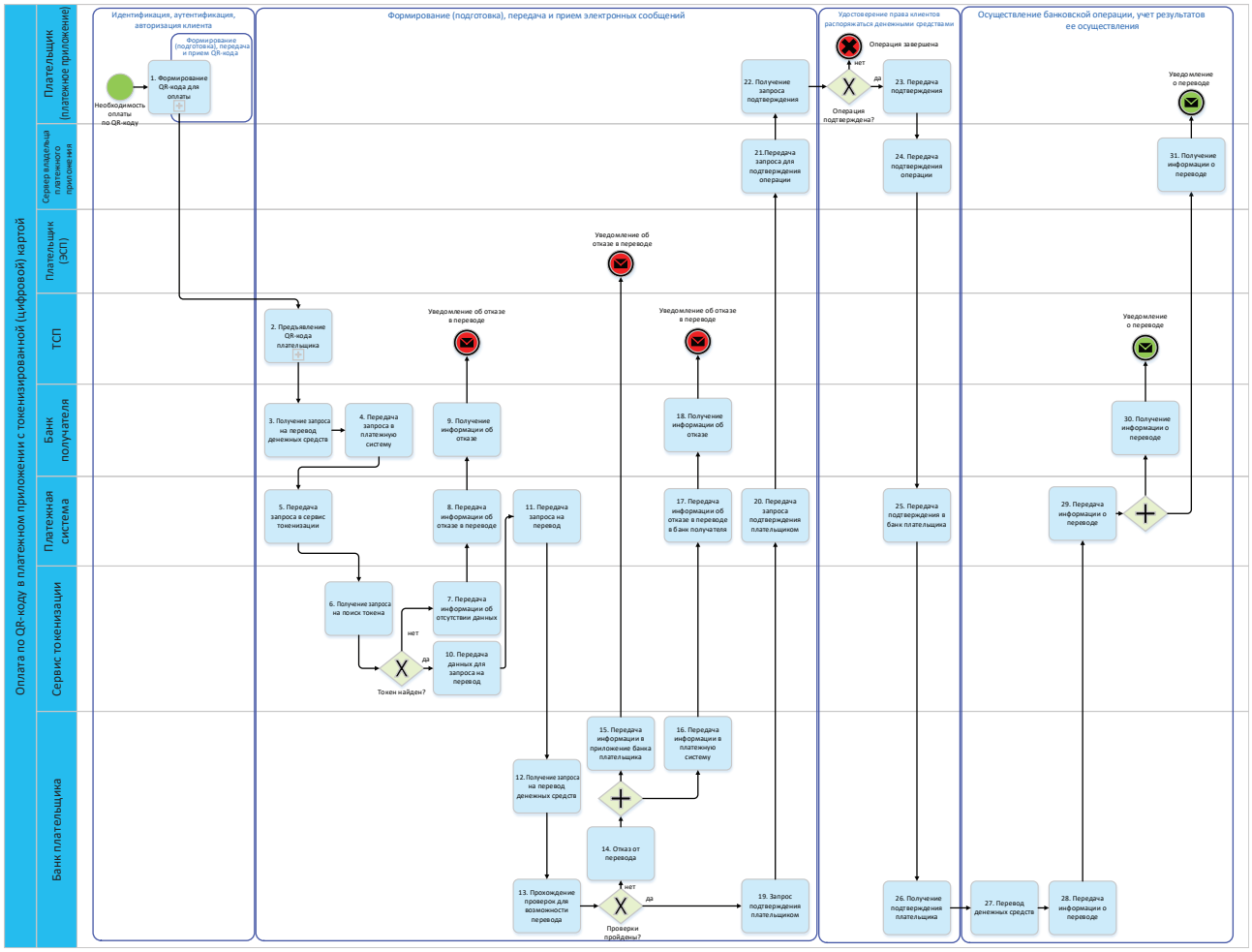
ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА В ПЛАТЕЖНОМ ПРИЛОЖЕНИИ *Рис. 22*



ПРЕДЪЯВЛЕНИЕ QR-КОДА ПЛАТЕЛЬЩИКОМ *Рис. 23*



ОПЛАТА ПО QR-КОДУ ПЛАТЕЛЬЩИКА В ПЛАТЕЖНОМ ПРИЛОЖЕНИИ *Рис. 24*



ПРИЛОЖЕНИЕ 7. ПРОЦЕСС СНЯТИЯ/ВНЕСЕНИЯ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ

Сценарий процесса

Пользователь с помощью платежного приложения формирует статический/динамический QR-код и представляет QR-код для сканирования банкоматом с целью снятия/внесения наличных денежных средств. Схема и описание формирования статического/динамического QR-кода на устройстве пользователя для снятия/внесения денежных средств представлены на рис. 21–22 процесса оплаты по QR-коду с использованием платежного приложения (приложение 6). Схема процесса предъявления QR-кода в банкомате приведена на рис. 18 процесса снятия/внесения денежных средств в банкомате через ЭСП (приложение 5).

Банкомат сканирует QR-код пользователя и передает запрос, чтобы проверить возможность списания денежных средств со счета в банк пользователя. Банк пользователя передает запрос в платежную систему, которая передает запрос на поиск данных карты для соответствующего токена в сервис токенизации. При положительном результате поиска сервис токенизации возвращает в банк пользователя через платежную систему данные по соответствующему токену. Банк пользователя передает запрос подтверждения операции на сервер поставщика платежного приложения, который передает запрос в платежное приложение. Пользователь подтверждает операцию и передает ответ на запрос через сервер поставщика платежного приложения в платежную систему. Платежная система передает ответ на запрос в банк пользователя, который проверяет корректность подтверждения пользователем. Банк пользователя уменьшает сумму денежных средств на счете, доступных пользователю для осуществления перевода, списывает денежные средства и передает уведомление о необходимости выдачи денежных средств в банкомат. Банкомат выдает денежные средства пользователю.

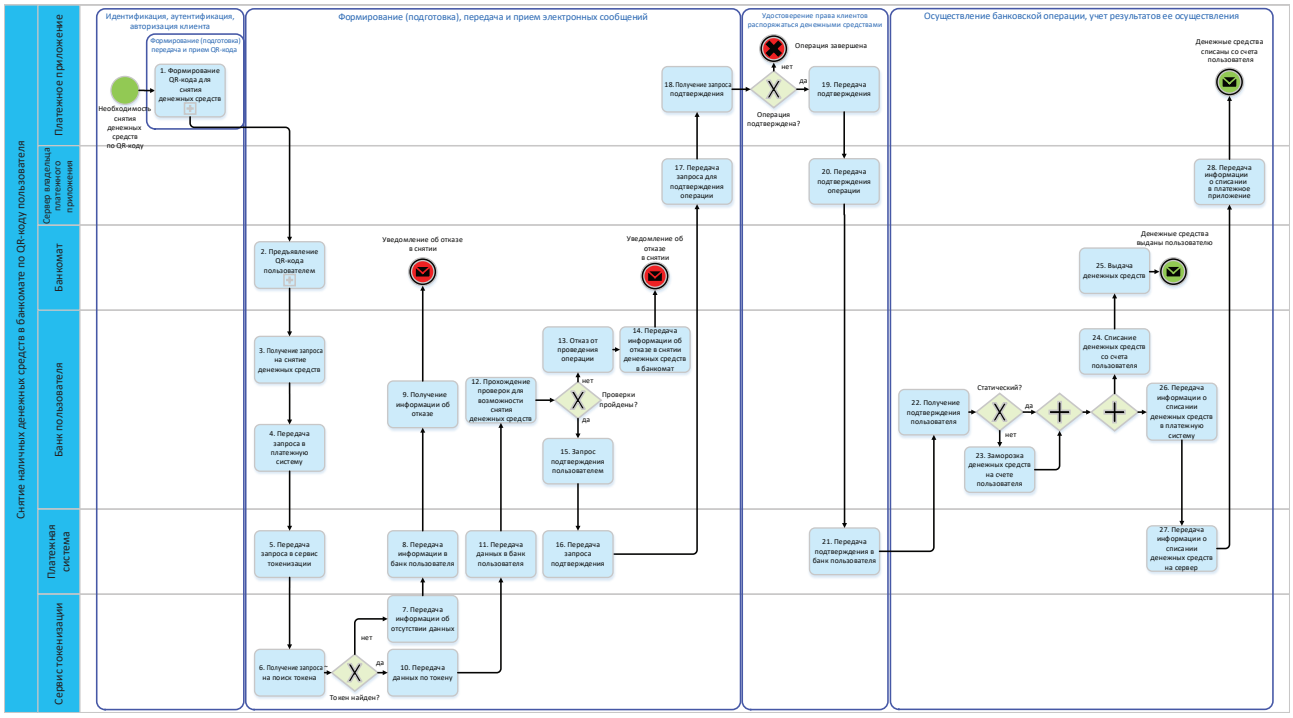
Банкомат сканирует QR-код пользователя и передает запрос, чтобы проверить возможность зачисления денежных средств на счет в банк пользователя. Банк пользователя передает запрос в платежную систему, которая передает запрос на поиск данных карты для соответствующего токена в сервис токенизации. При положительном результате поиска сервис токенизации возвращает в банк пользователя через платежную систему данные по соответствующему токену. Банк пользователя передает запрос подтверждения операции на сервер поставщика платежного приложения, который передает запрос в платежное приложение. Пользователь подтверждает операцию и передает ответ на запрос через сервер поставщика платежного приложения в платежную систему. Платежная система передает ответ на запрос в банк пользователя, который проверяет корректность подтверждения пользователем. Банк пользователя передает уведомление в банкомат о возможности внесения денежных средств пользователем. Банкомат передает информацию о необходимости зачисления денежных средств на счет.

Схемы процесса представлены на рис. 25, 26. Меры защиты на технологических участках и подэтапах перечислены в табл. 14.

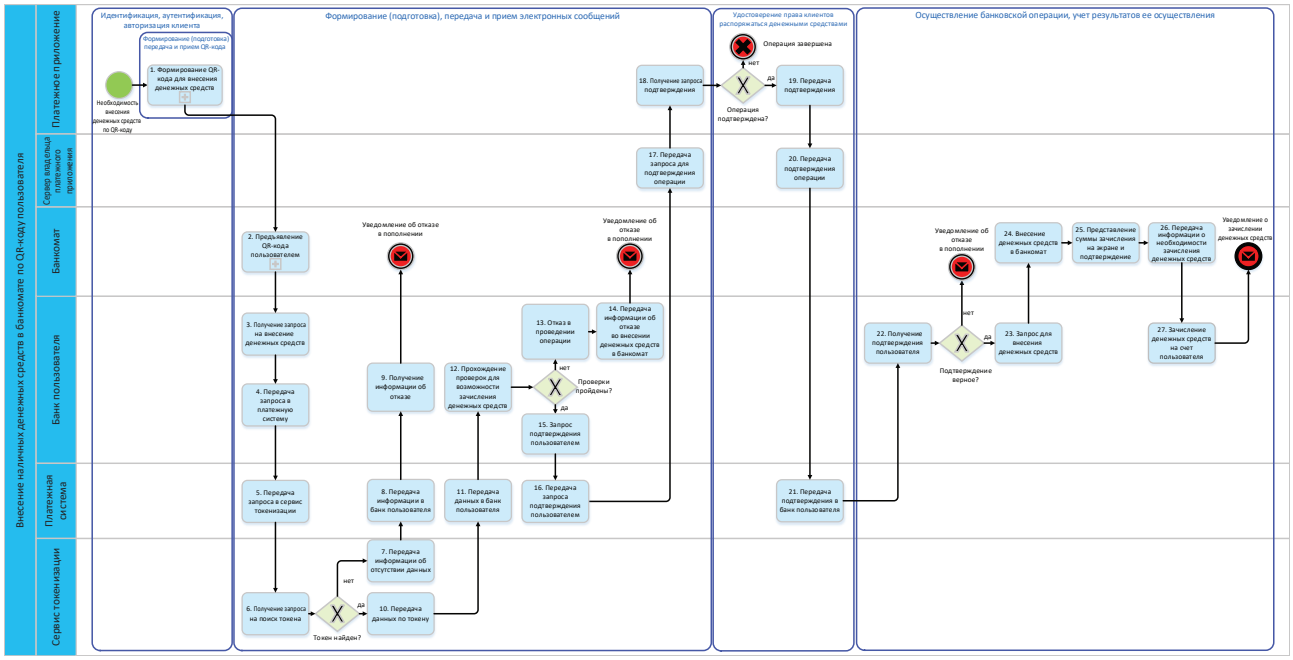
МЕРЫ ЗАЩИТЫ ПРИ СНЯТИИ/ВНЕСЕНИИ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ В БАНКОМАТЕ *Табл. 14*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 3.2.4

СНЯТИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ ПО QR-КОДУ ПОЛЬЗОВАТЕЛЯ *Рис. 25*



ВНЕСЕНИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ ПО QR-КОДУ ПОЛЬЗОВАТЕЛЯ *Рис. 26*



ПРИЛОЖЕНИЕ 8. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ ТСП

Сценарий процесса

Получатель в приложении вводит сумму покупки/услуги и запрашивает QR-код в динамическом сценарии у поставщика платежного QR-кода (банк получателя). Полученный QR-код представляется плательщику на POS-терминале.

Плательщик проходит аутентификацию в ЭСП, сканирует QR-код на POS-терминале, выбирает платежную карту, привязанную к счету, с которого будут списаны денежные средства, и передает запрос на перевод денежных средств в банк плательщика.

Банк плательщика проводит проверки по счету плательщика на возможность осуществления перевода денежных средств, при положительном результате передается запрос через платежную систему в банк получателя.

Банк получателя проводит проверки по счету получателя на возможность осуществления перевода денежных средств, при положительном результате передается ответ на запрос через платежную систему в банк плательщика. Банк плательщика списывает денежные средства со счета плательщика, банк получателя зачисляет денежные средства на счет получателя.

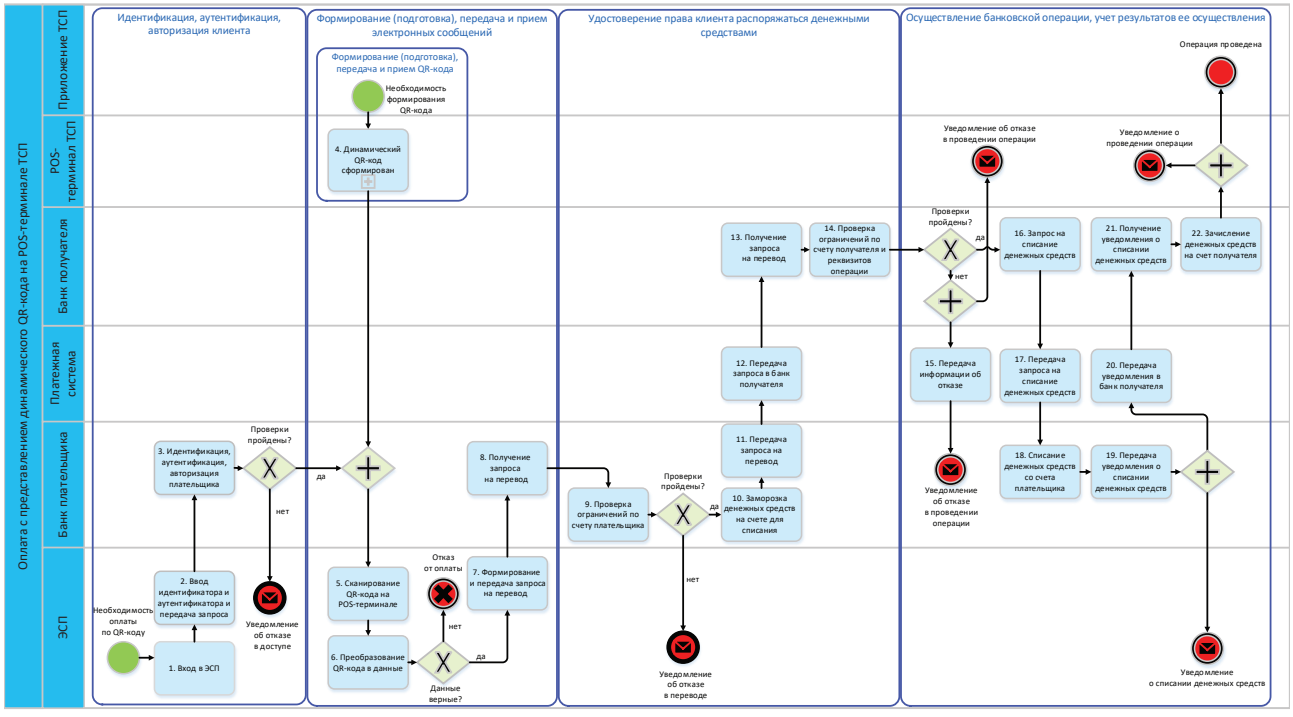
Схемы процесса представлены на рис. 27, 28. Меры защиты на технологических участках и подэтапах приведены в табл. 15.

МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО ДИНАМИЧЕСКОМУ QR-КОДУ НА POS-ТЕРМИНАЛЕ *Табл. 15*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.3.4, 2.5.1, 2.5.2, 3.1.5
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.4.1, 2.3.2, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 3.2.4

ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ *Рис. 27*

ОПЛАТА С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ *Рис. 28*



ПРИЛОЖЕНИЕ 9. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА КАССЕ ТСП (ЭКРАН ПРОДАВЦА) – МОНИТОР, ПЛАНШЕТ, ТЕЛЕФОН

Сценарий процесса

Получатель в приложении формирует запрос поставщику платежного QR-кода (банк получателя) на получение QR-кода в статическом сценарии. Полученный QR-код в статическом сценарии представляется плательщику на POS-терминале для оплаты.

Плательщик проходит аутентификацию в ЭСП, сканирует QR-код на POS-терминале, выбирает реквизиты, откуда будут списаны денежные средства, вводит сумму и передает запрос на перевод денежных средств в банк плательщика.

Банк плательщика проводит проверки по счету плательщика на возможность осуществления перевода денежных средств, при положительном результате передается запрос через платежную систему в банк получателя.

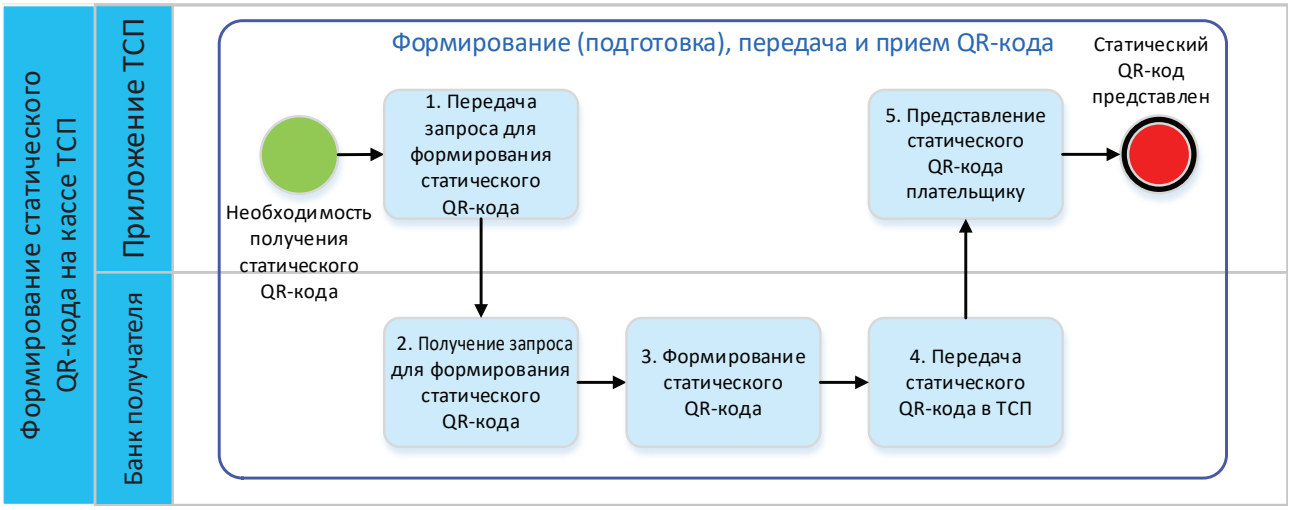
Банк получателя проводит проверки по счету получателя на возможность осуществления перевода денежных средств, при положительном результате передается ответ на запрос через платежную систему в банк плательщика. Банк плательщика списывает денежные средства со счета плательщика, банк получателя средств зачисляет денежные средства на счет получателя.

Схемы процесса представлены на рис. 29, 30. Меры защиты на технологических участках и подэтапах приведены в табл. 16.

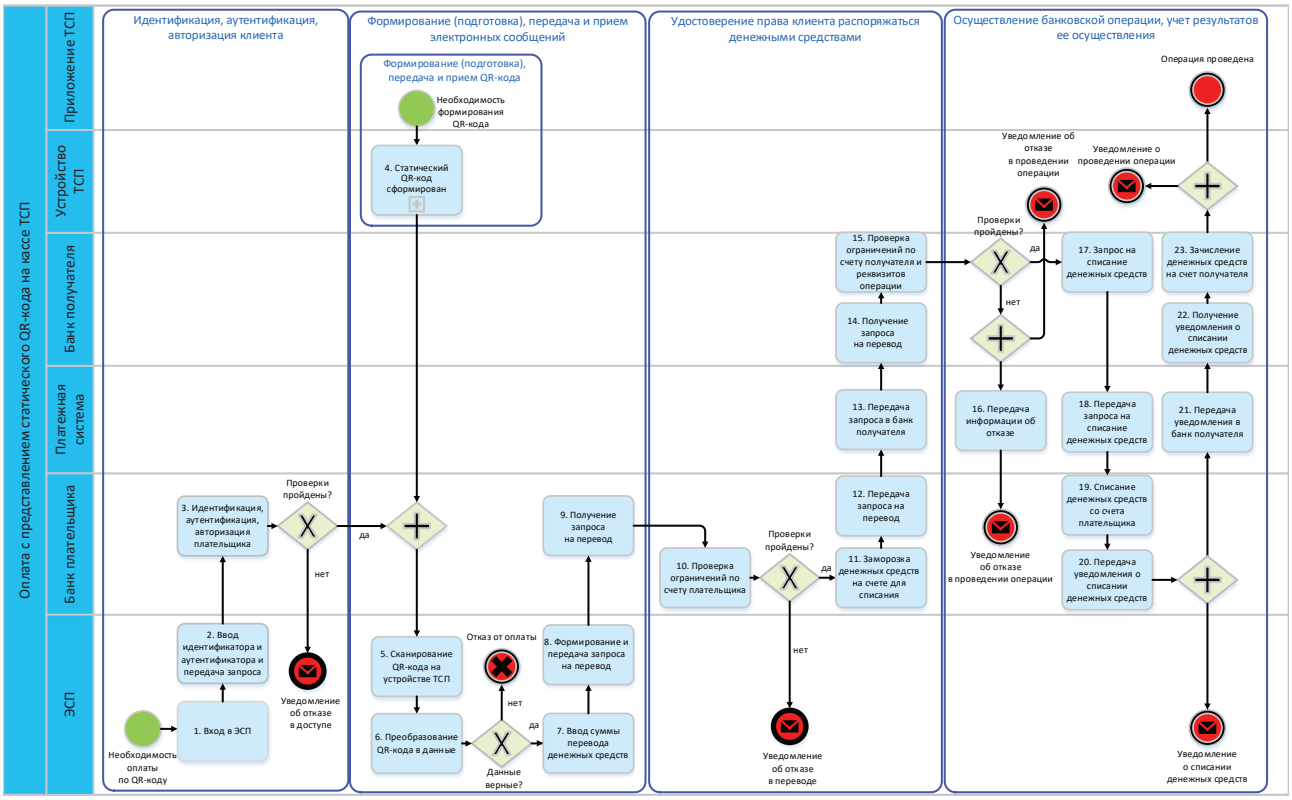
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО СТАТИЧЕСКОМУ QR-КОДУ НА КАССЕ ТСП *Табл. 16*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1, 3.1.2, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА НА КАССЕ ТСП *Рис. 29*



ОПЛАТА С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА КАССЕ ТСП (ЭКРАН ПРОДАВЦА) *Рис. 30*



ПРИЛОЖЕНИЕ 10. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА КАССЕ ТСП (ЭКРАН ПРОДАВЦА) – МОНИТОР, ПЛАНШЕТ, ТЕЛЕФОН

Сценарий процесса

Получатель в приложении формирует запрос поставщику платежного QR-кода (банк получателя) на получение QR-кода в динамическом сценарии. Полученный QR-код в динамическом сценарии представляется плательщику на POS-терминале для оплаты.

Плательщик проходит аутентификацию в ЭСП, сканирует QR-код на POS-терминале, выбирает реквизиты, откуда будут списаны денежные средства и передает запрос на перевод денежных средств в банк плательщика.

Банк плательщика проводит проверки по счету плательщика на возможность осуществления перевода денежных средств, при положительном результате передается запрос через платежную систему в банк получателя.

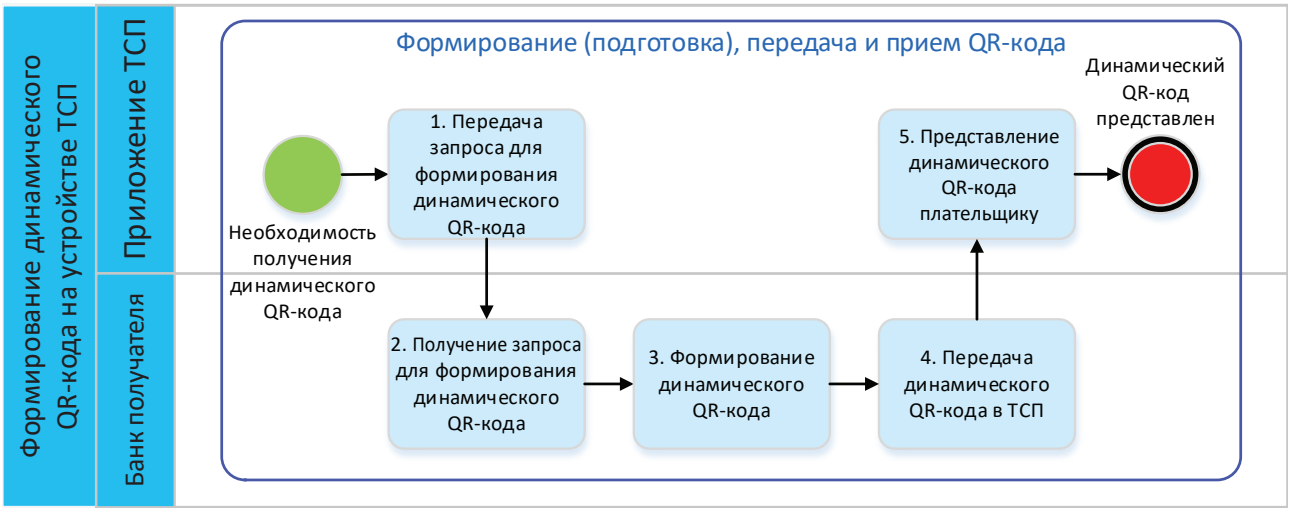
Банк получателя проводит проверки по счету получателя на возможность осуществления перевода денежных средств, при положительном результате передается ответ на запрос через платежную систему в банк плательщика. Банк плательщика списывает денежные средства со счета плательщика, банк получателя средств зачисляет денежные средства на счет получателя.

Схемы процесса представлены на рис. 31, 32. Меры защиты на технологических участках и подэтапах приведены в табл. 17.

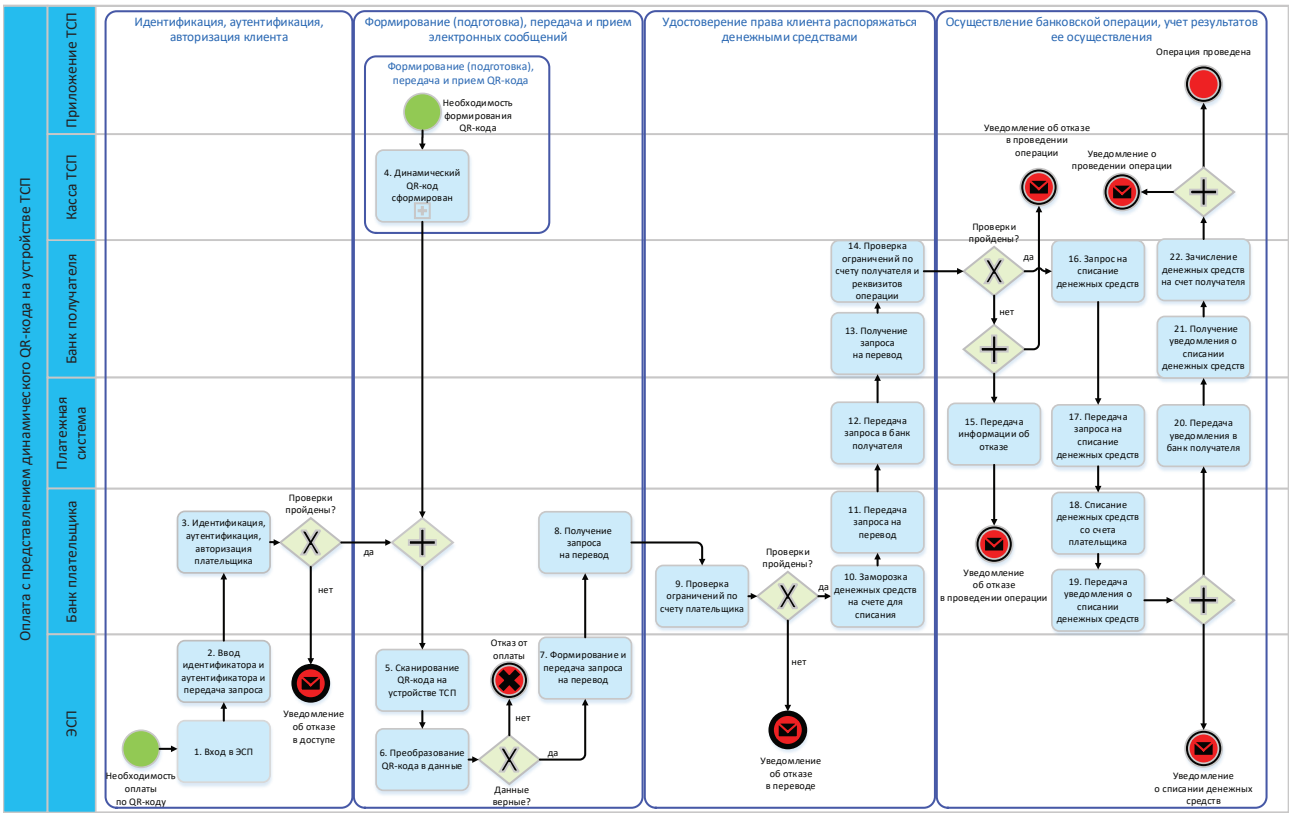
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО ДИНАМИЧЕСКОМУ QR-КОДУ НА КАССЕ *Табл. 17*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА НА УСТРОЙСТВЕ ТСП *Рис. 31*



ОПЛАТА С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА УСТРОЙСТВЕ ТСП *Рис. 32*



ПРИЛОЖЕНИЕ 11. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ В ТСП (НАКЛЕЙКА)

Сценарий процесса

Получатель в приложении формирует запрос поставщику платежного QR-кода (банк получателя) на получение QR-кода в статическом сценарии. Полученный QR-код в статическом сценарии получатель печатает и размещает в ТСП для возможности оплаты плательщиком.

Плательщик проходит аутентификацию в ЭСП, сканирует распечатанный QR-код, выбирает платежную карту, привязанную к счету, с которого будут списаны денежные средства, вводит сумму и передает запрос на перевод денежных средств в банк плательщика.

Банк плательщика проводит проверки по счету плательщика на возможность осуществления перевода денежных средств, при положительном результате передается запрос через платежную систему в банк получателя.

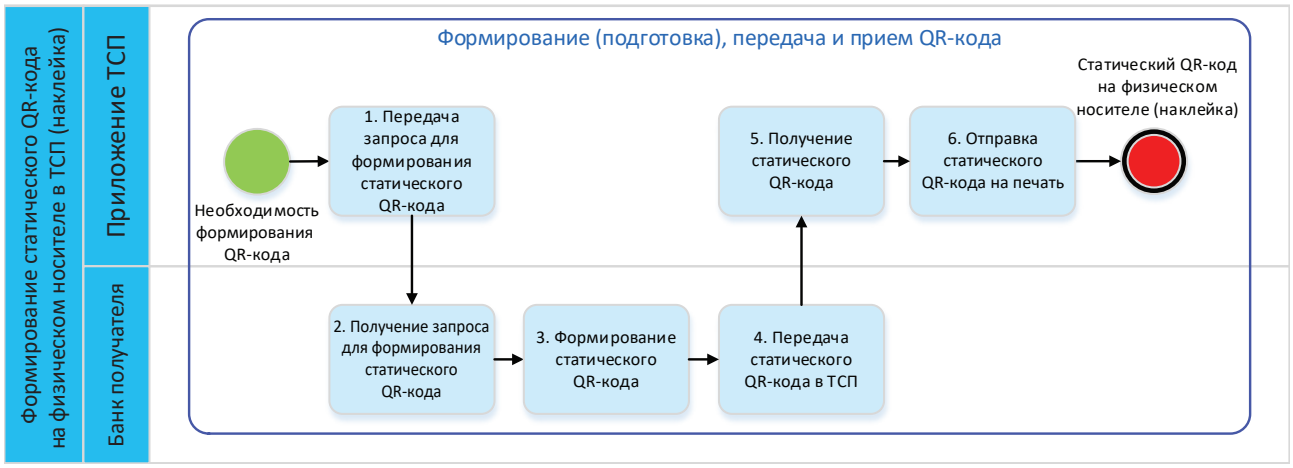
Банк получателя проводит проверки по счету получателя на возможность осуществления перевода денежных средств, при положительном результате передается ответ на запрос через платежную систему в банк плательщика. Банк плательщика списывает денежные средства со счета плательщика, банк получателя зачисляет денежные средства на счет получателя.

Схемы процесса представлены на рис. 33, 34. Меры защиты на технологических участках и подэтапах приведены в табл. 18.

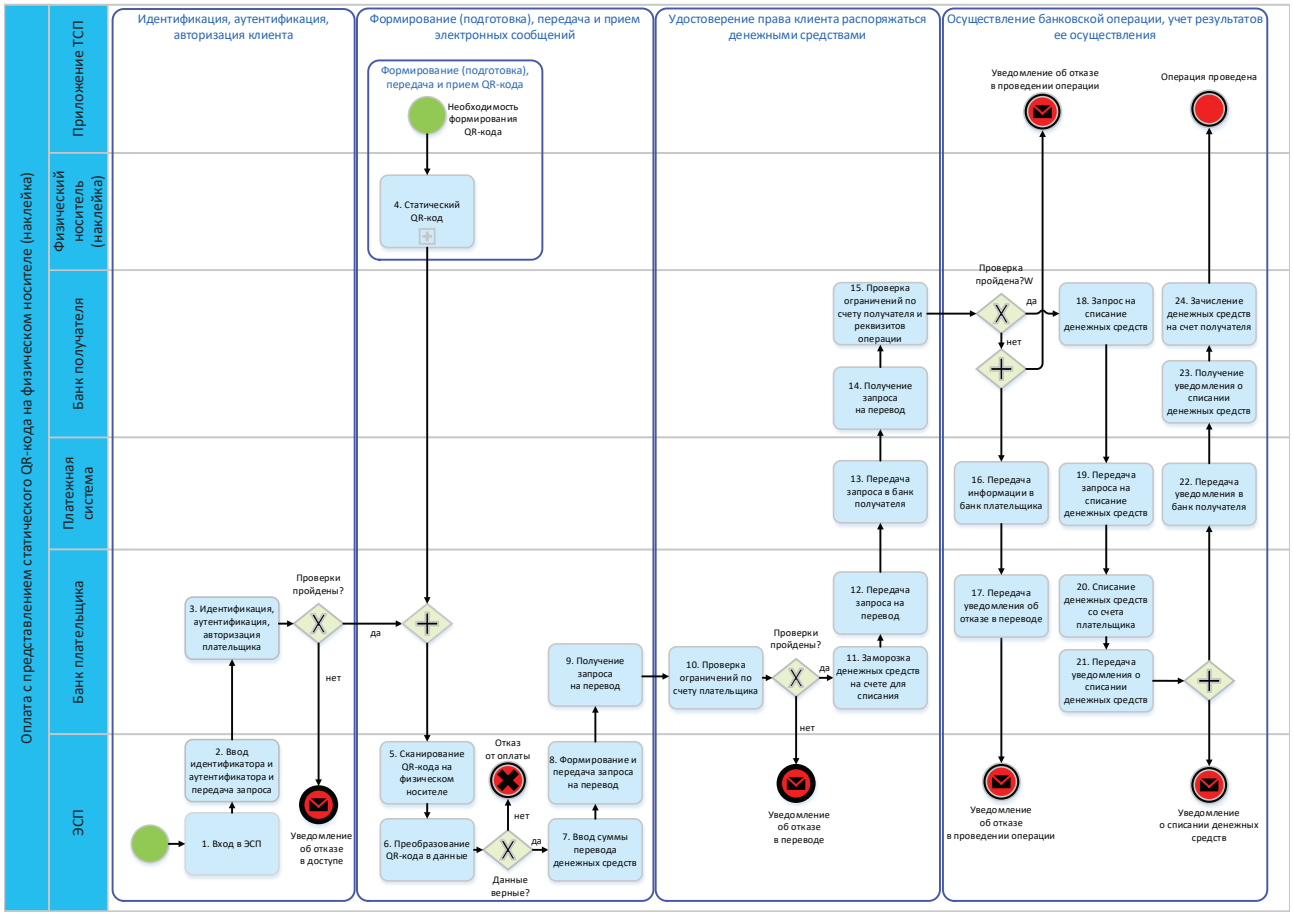
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО СТАТИЧЕСКОМУ QR-КОДУ НА ФИЗИЧЕСКОМ НОСИТЕЛЕ *Табл. 18*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.1, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	1.1.6, 2.3.7, 3.1.4, 3.4.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1, 3.1.2, 3.1.7, 3.1.8
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ В ТСП (НАКЛЕЙКА) *Рис. 33*



ОПЛАТА С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ (НАКЛЕЙКА) *Рис. 34*



ПРИЛОЖЕНИЕ 12. ПРОЦЕСС ОПЛАТЫ В ФИНТЕХПРИЛОЖЕНИИ ПО QR-КОДУ

Сценарий процесса

Получатель в приложении формирует запрос поставщику платежного QR-кода (банк получателя) на получение QR-кода в статическом сценарии. Полученный QR-код в статическом сценарии получатель размещает в финтехприложении для возможности оплаты плательщиком.

Плательщик проходит аутентификацию в финтехприложении, нажимает на QR-код, переходит в ЭСП банка плательщика, выбирает реквизиты, откуда будут списаны денежные средства, вводит сумму, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика.

Банк плательщика проверяет счет плательщика на возможность осуществления перевода денежных средств, при положительном результате передается запрос через платежную систему в банк получателя.

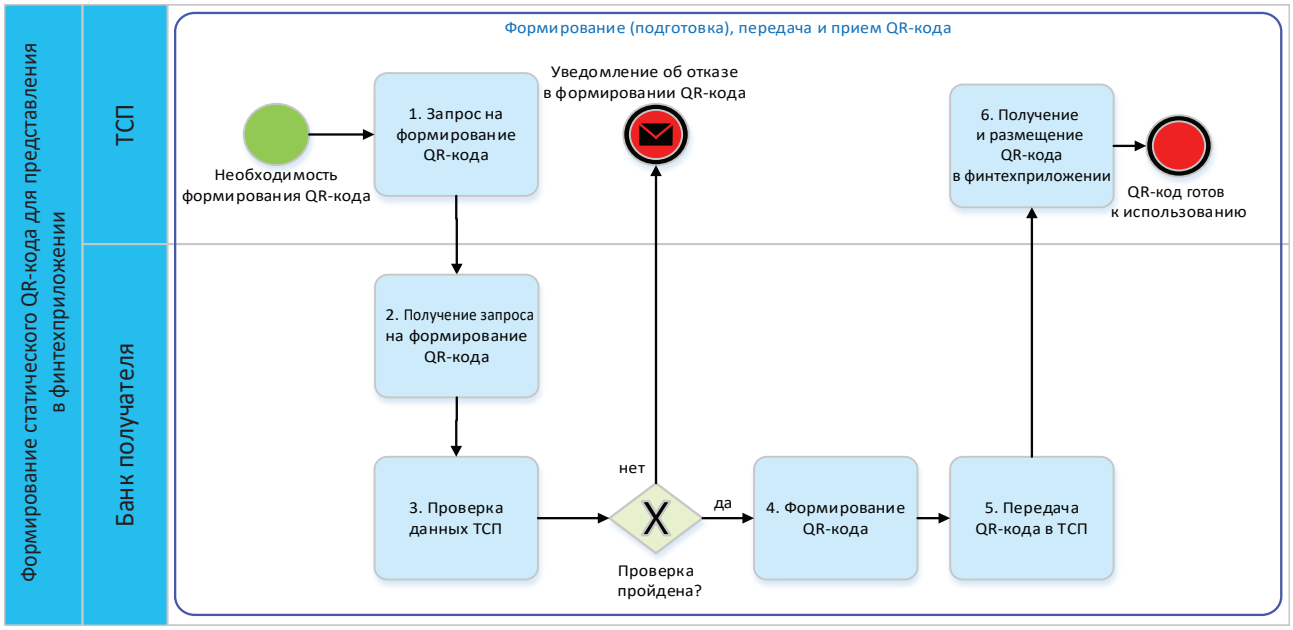
Банк получателя проверяет счет получателя на возможность осуществления перевода денежных средств, при положительном результате проверок передается ответ на запрос через платежную систему в банк плательщика. Банк плательщика списывает денежные средства со счета плательщика, банк получателя зачисляет денежные средства на счет получателя.

Схемы процесса представлены на рис. 35–37. Меры защиты на технологических участках и подэтапах приведены в табл. 19.

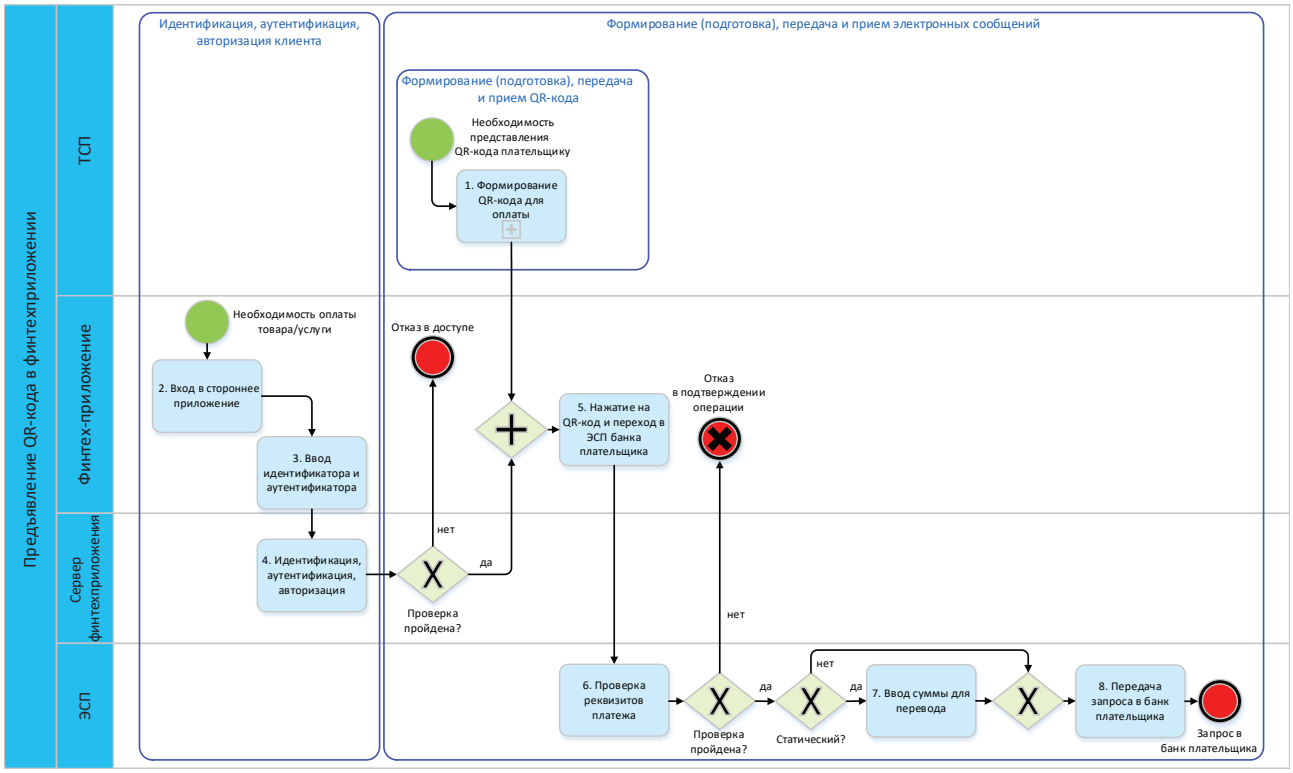
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО QR-КОДУ В ФИНТЕХПРИЛОЖЕНИИ *Табл. 19*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	2.3.7, 3.1.4, 3.1.5
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.4.2, 3.2.4

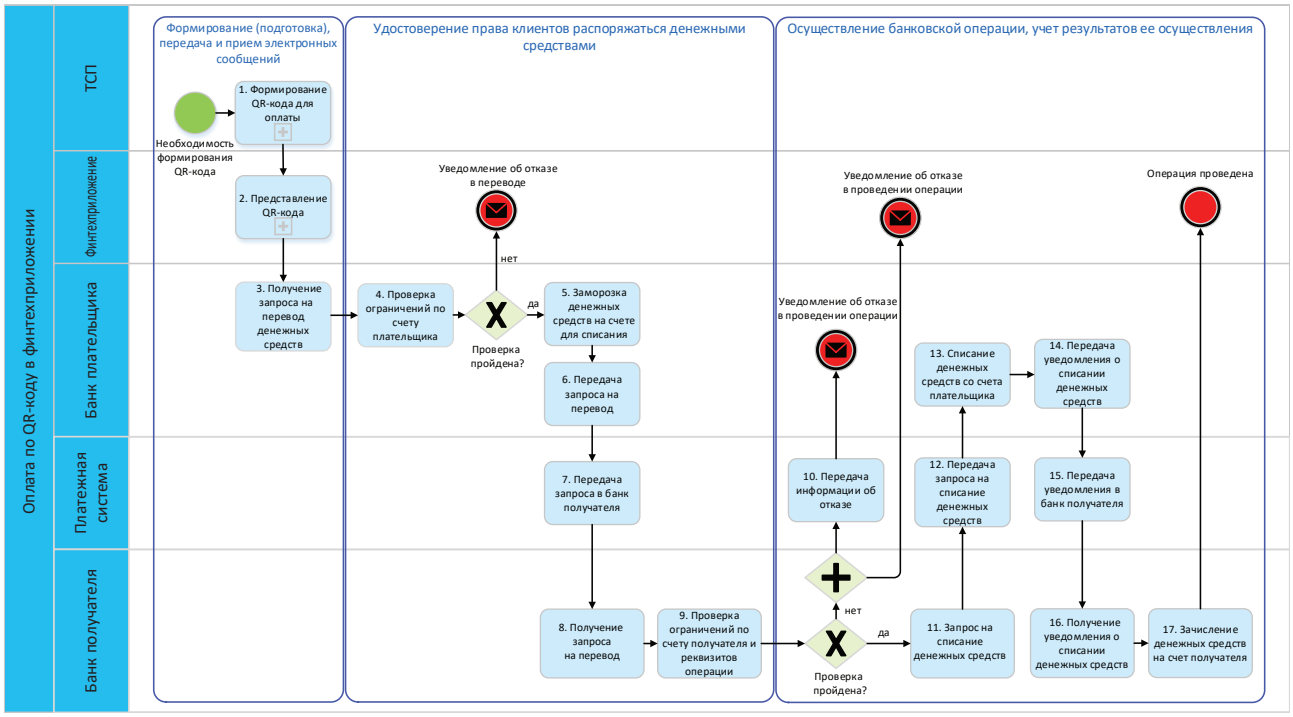
ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ В ФИНТЕХПРИЛОЖЕНИИ *Рис. 35*



ПРЕДЪЯВЛЕНИЕ QR-КОДА В ФИНТЕХПРИЛОЖЕНИИ *Рис. 36*



ОПЛАТА ПО QR-КОДУ В ФИНТЕХПРИЛОЖЕНИИ *Рис. 37*



ПРИЛОЖЕНИЕ 13. ПРОЦЕСС СНЯТИЯ/ВНЕСЕНИЯ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО QR-КОДА В БАНКОМАТЕ

Сценарий процесса

Пользователь в банкомате выбирает опцию снятия/внесения денежных средств по QR-коду. Банкомат передает запрос в банк пользователя на формирование QR-кода в динамическом сценарии.

Пользователь проходит аутентификацию в ЭСП, после которой сканирует QR-код банкомата, выбирает в ЭСП карту, вводит сумму снятия денежных средств и передает запрос в банк пользователя. Банк пользователя проверяет возможность снятия денежных средств и при положительном результате передает в платежное приложение пользователя запрос подтверждения. Пользователь подтверждает операцию. Банк пользователя проверяет корректность подтверждения плательщиком, уменьшает сумму денежных средств, доступных пользователю для осуществления перевода, после чего происходит списание денежных средств и передача уведомления в банкомат о необходимости выдачи денежных средств пользователю.

Пользователь проходит аутентификацию в ЭСП, после чего сканирует QR-код банкомата, выбирает в ЭСП карту для внесения денежных средств и передает запрос в банк пользователя. Банк пользователя проверяет возможность внесения денежных средств и при положительном результате передает в ЭСП пользователя запрос подтверждения. Пользователь подтверждает операцию. Банк пользователя проверяет корректность подтверждения пользователем и передает уведомление в банкомат на внесение денежных средств. После внесения денежных средств пользователем банкомат передает уведомление в банк пользователя о необходимости зачисления денежных средств на счет.

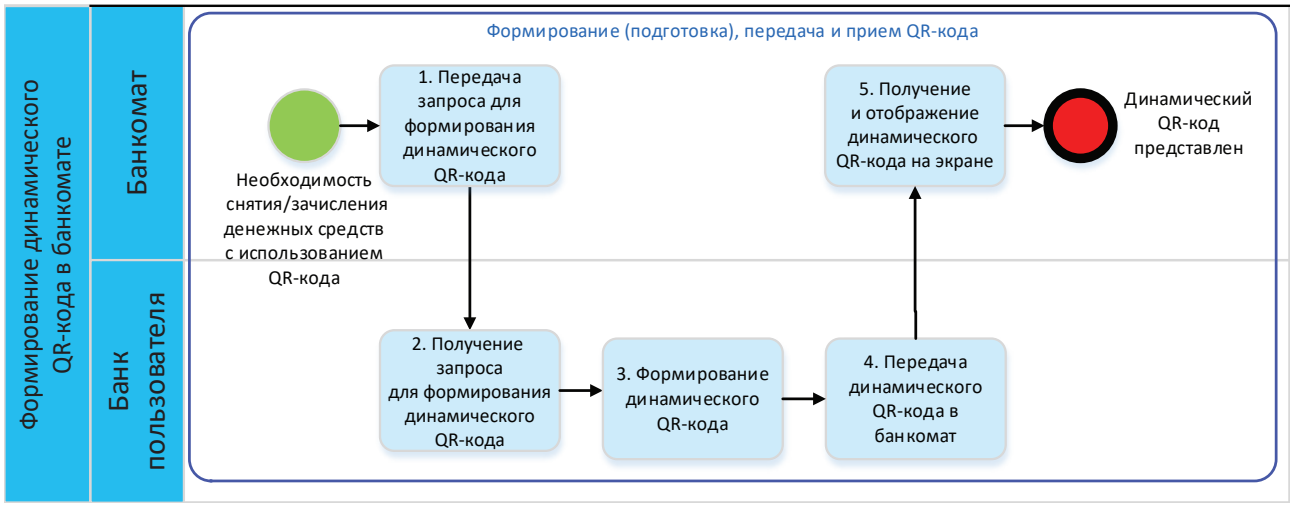
Схемы процесса представлены на рис. 38–40. Меры защиты на технологических участках и подэтапах приведены в табл. 20.

МЕРЫ ЗАЩИТЫ ПРИ СНЯТИИ/ВНЕСЕНИИ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО QR-КОДА В БАНКОМАТЕ *Табл. 20*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.3.4, 2.5.1, 2.5.2, 3.1.5, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4
5	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	1.1.6, 2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.4.2, 3.2.4

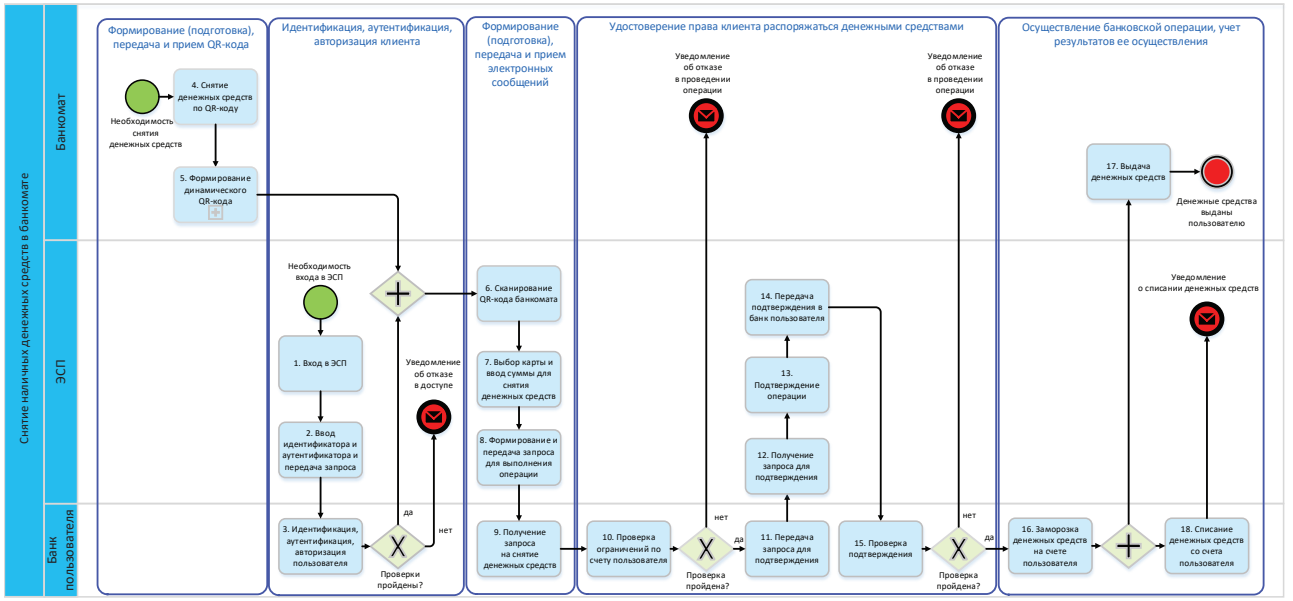
ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА В БАНКОМАТЕ

Рис. 38



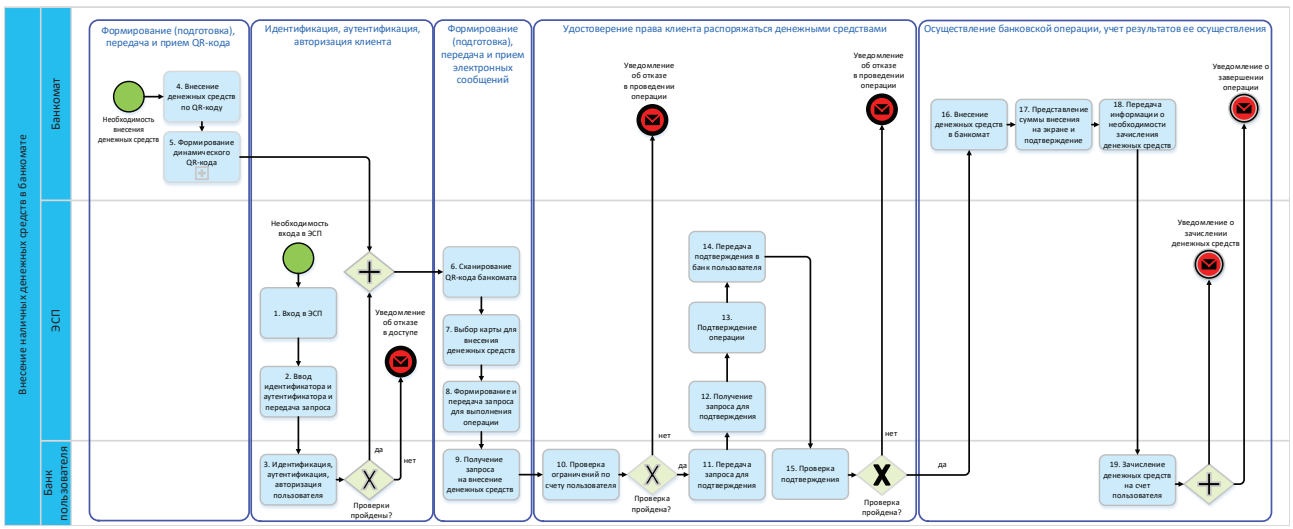
СНЯТИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ

Рис. 39



ВНЕСЕНИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В БАНКОМАТЕ

Рис. 40



ПРИЛОЖЕНИЕ 14. ПРОЦЕСС ОПЛАТЫ С ПРЕДСТАВЛЕНИЕМ QR-КОДА В КВИТАНЦИИ (БУМАЖНЫЙ НОСИТЕЛЬ)

Сценарий процесса

Получатель в прикладном ПО организации заполняет реквизиты операции перевода денежных средств, формирует QR-код в статическом сценарии и печатает его в квитанции для перевода денежных средств плательщиком.

Плательщик проходит аутентификацию в ЭСП, сканирует QR-код, выбирает карту, привязанную к счету, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика.

Банк плательщика проверяет счет плательщика на возможность осуществления перевода денежных средств, при положительном результате передается запрос через платежную систему в банк получателя.

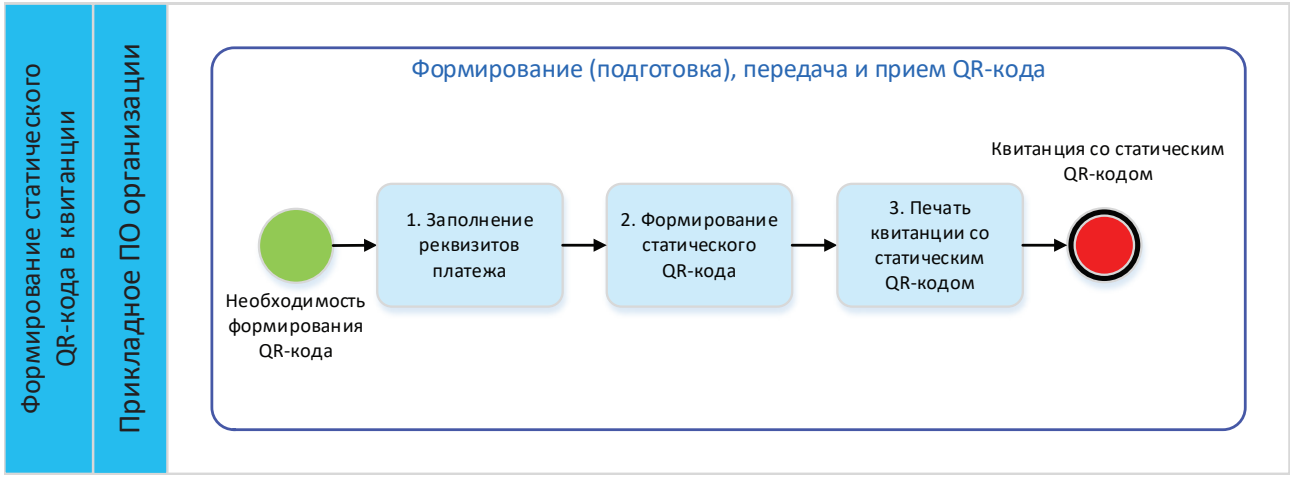
Банк получателя проверяет счет получателя на возможность осуществления перевода денежных средств, при положительном результате проверки передается ответ на запрос через платежную систему в банк плательщика. Банк плательщика списывает денежные средства со счета плательщика, банк получателя зачисляет денежные средства на счет получателя.

Схемы процесса представлены на рис. 41, 42. Меры защиты на технологических участках и подэтапах приведены в табл. 21.

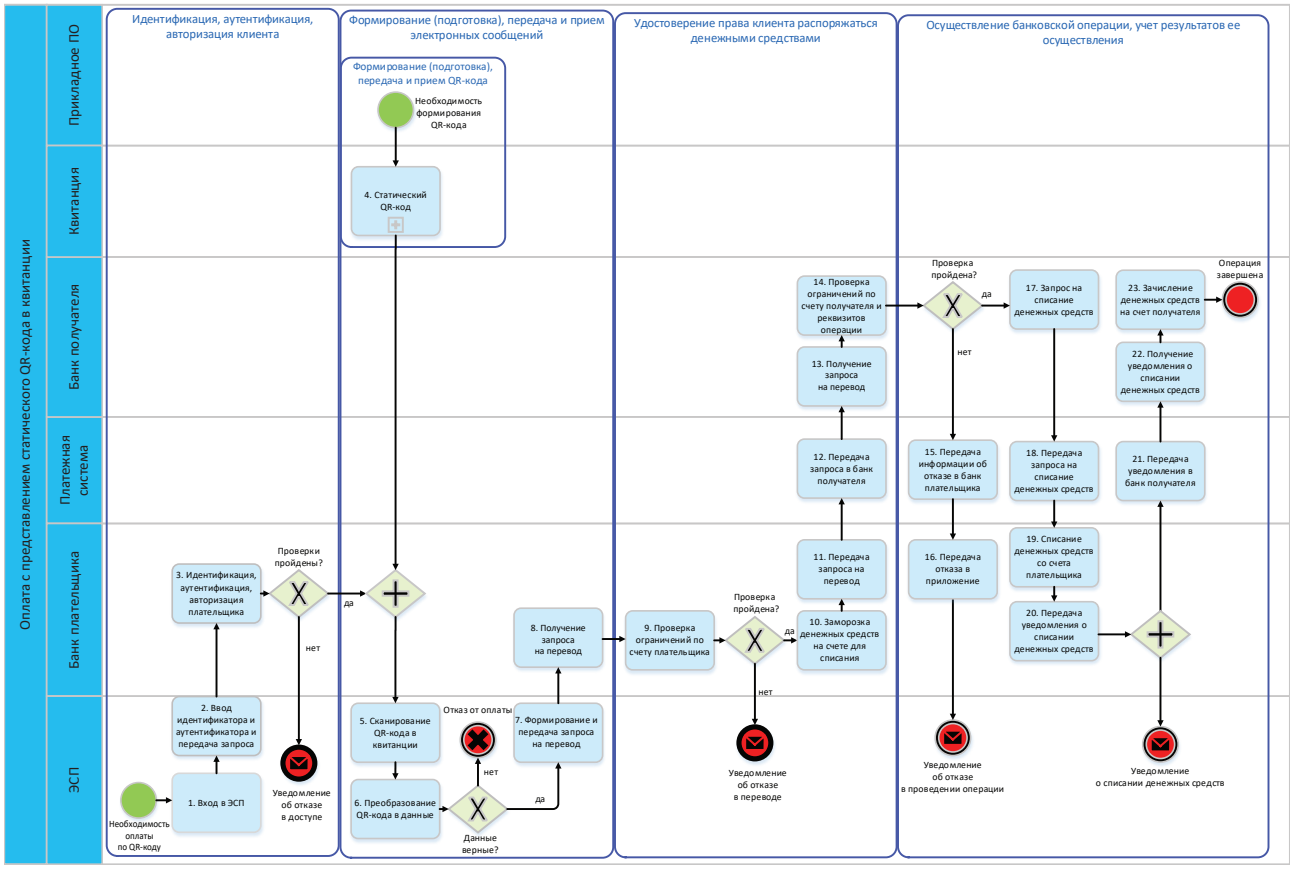
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО QR-КОДУ В КВИТАНЦИИ *Табл. 21*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.2, 2.5.1, 2.5.2, 3.1.5, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	2.1.1
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
5.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.7, 3.1.4
6.	Осуществление банковской операции, учет результатов ее осуществления	3.1.2, 3.1.7, 3.1.8
7.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА В КВИТАНЦИИ *Рис. 41*



ОПЛАТА С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА В КВИТАНЦИИ *Рис. 42*



ПРИЛОЖЕНИЕ 15. ПРОЦЕСС ОПЛАТЫ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА КАССЕ ТСП (НАКЛЕЙКА)

Сценарий процесса

ТСП формирует и передает запрос на QR-код в статическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП (QR-код в статическом сценарии заранее сформирован). ТСП печатает QR-код для предоставления плательщику.

ТСП в приложении вводит сумму платежа и передает запрос на активацию QR-кода агенту ТСП, агент ТСП передает запрос в ОПКЦ СБП. ОПКЦ СБП активирует QR-код и передает уведомление в приложение ТСП через агента ТСП. QR-код в статическом сценарии активен.

Плательщик проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика. Далее – типовой процесс C2B СБП, регламентированный в стандартах ОПКЦ СБП.

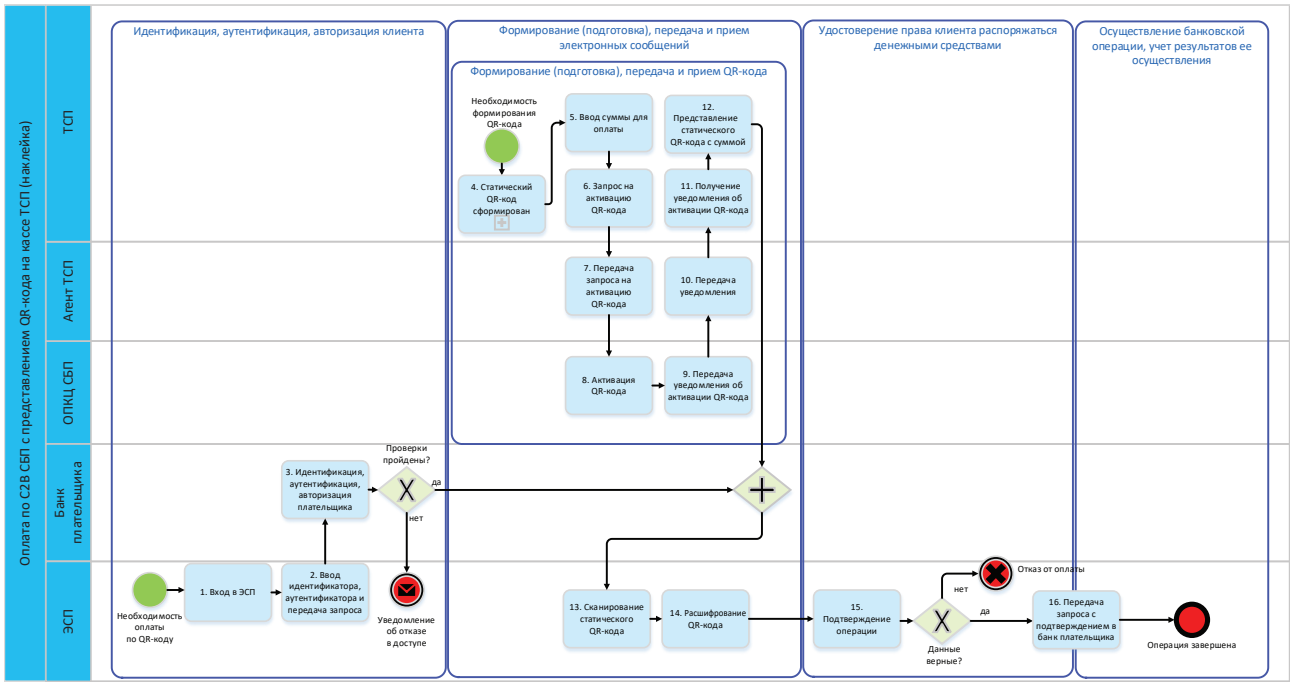
Схемы процесса представлены на рис. 43, 44. Меры защиты на технологических участках и подэтапах приведены в табл. 22.

МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА КАССЕ *Табл. 22*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.1, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1, 3.1.2, 3.1.7, 3.1.8
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА КАССЕ ТСП (НАКЛЕЙКА) *Рис. 43*

ОПЛАТА ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ QR-КОДА НА КАССЕ ТСП (НАКЛЕЙКА) *Рис. 44*



ПРИЛОЖЕНИЕ 16. ПРОЦЕСС ОПЛАТЫ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ

Сценарий процесса

ТСП формирует и передает запрос на QR-код в статическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП (QR-код в статическом сценарии заранее сформирован).

ТСП в приложении вводит сумму платежа и передает запрос на активацию QR-кода агенту ТСП, агент ТСП передает запрос в ОПКЦ СБП. ОПКЦ СБП активирует QR-код и передает уведомление в приложение ТСП через агента ТСП. QR-код в статическом сценарии активен и представлен на POS-терминале.

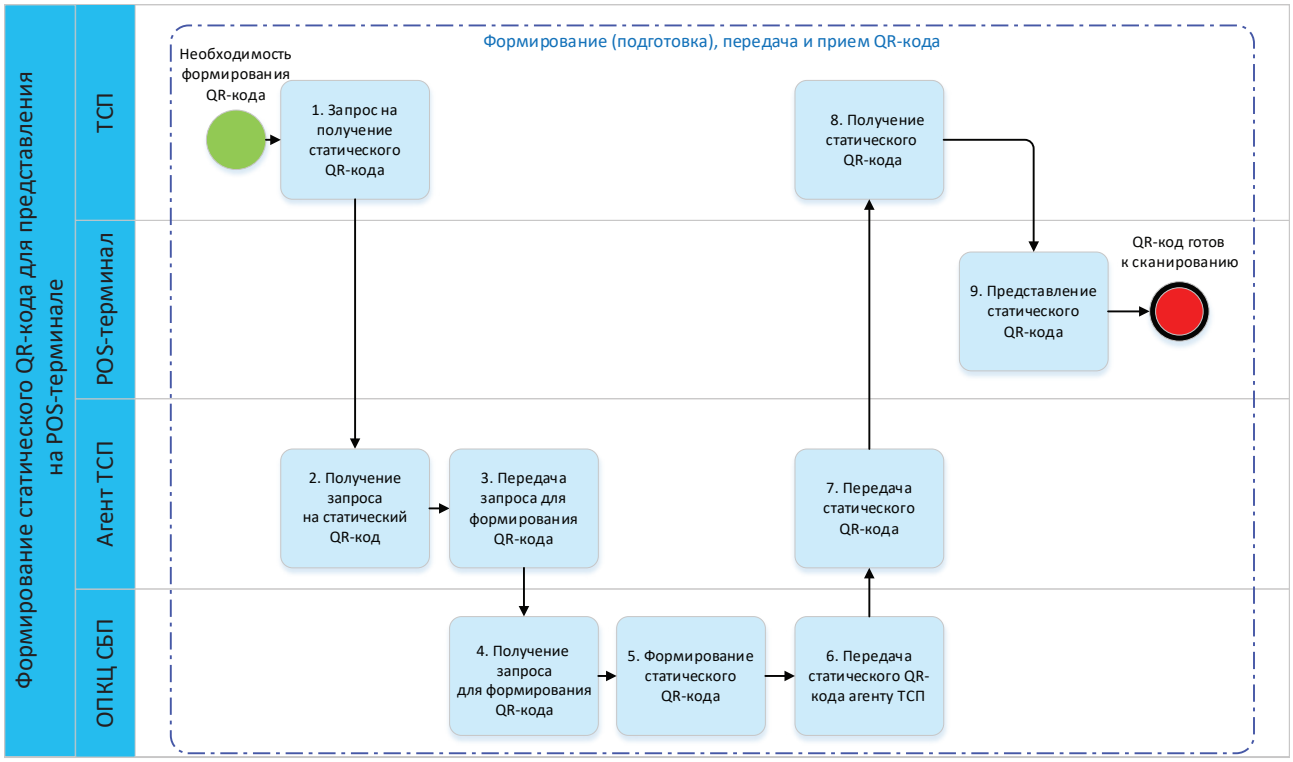
Плательщик проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на осуществление перевода денежных средств в банк плательщика. Далее – типовой процесс C2B СБП, регламентированный в стандартах ОПКЦ СБП.

Схемы процесса представлены на рис. 45, 46. Меры защиты на технологических участках и подэтапах приведены в табл. 23.

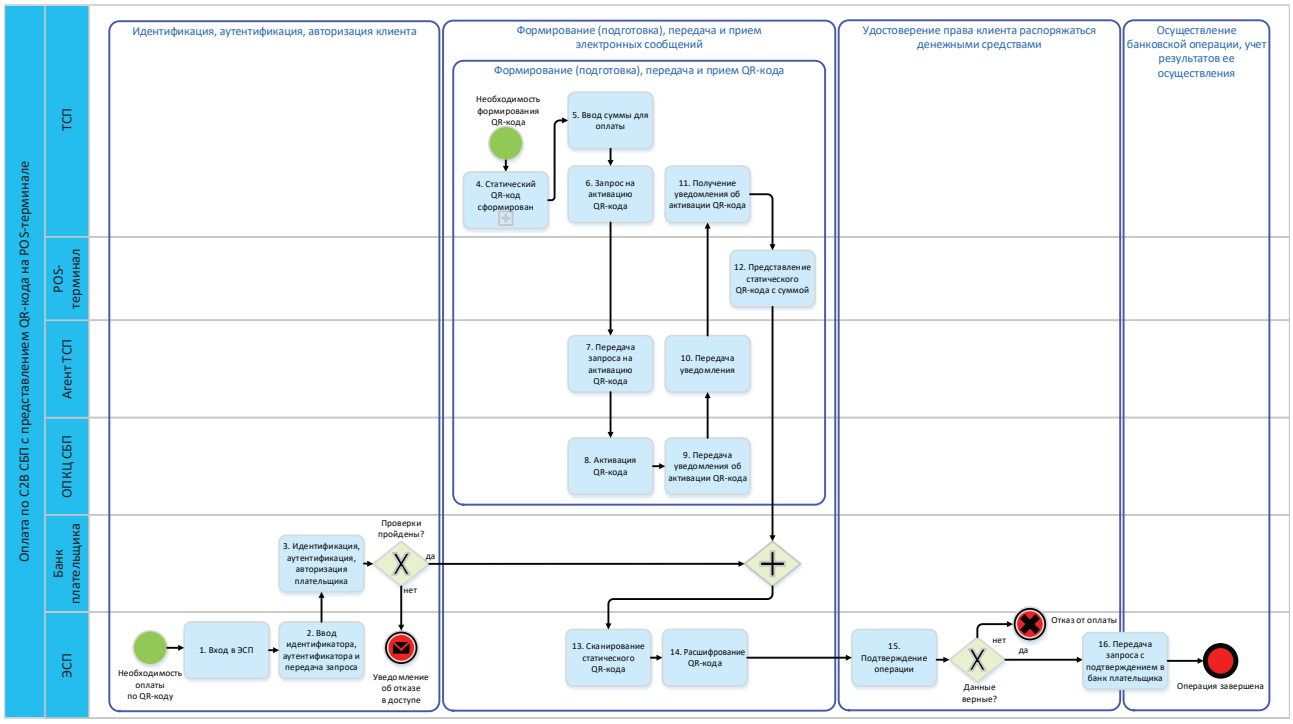
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ *Табл. 23*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2, 3.4.4
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	2.4.3, 3.1.1, 3.1.2, 3.1.7, 3.1.8
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА POS-ТЕРМИНАЛЕ *Рис. 45*



ОПЛАТА ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ *Рис. 46*



ПРИЛОЖЕНИЕ 17. ПРОЦЕСС ОПЛАТЫ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ

Сценарий процесса

ТСП формирует и передает запрос на QR-код в динамическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП. QR-код в динамическом сценарии представлен на POS-терминале.

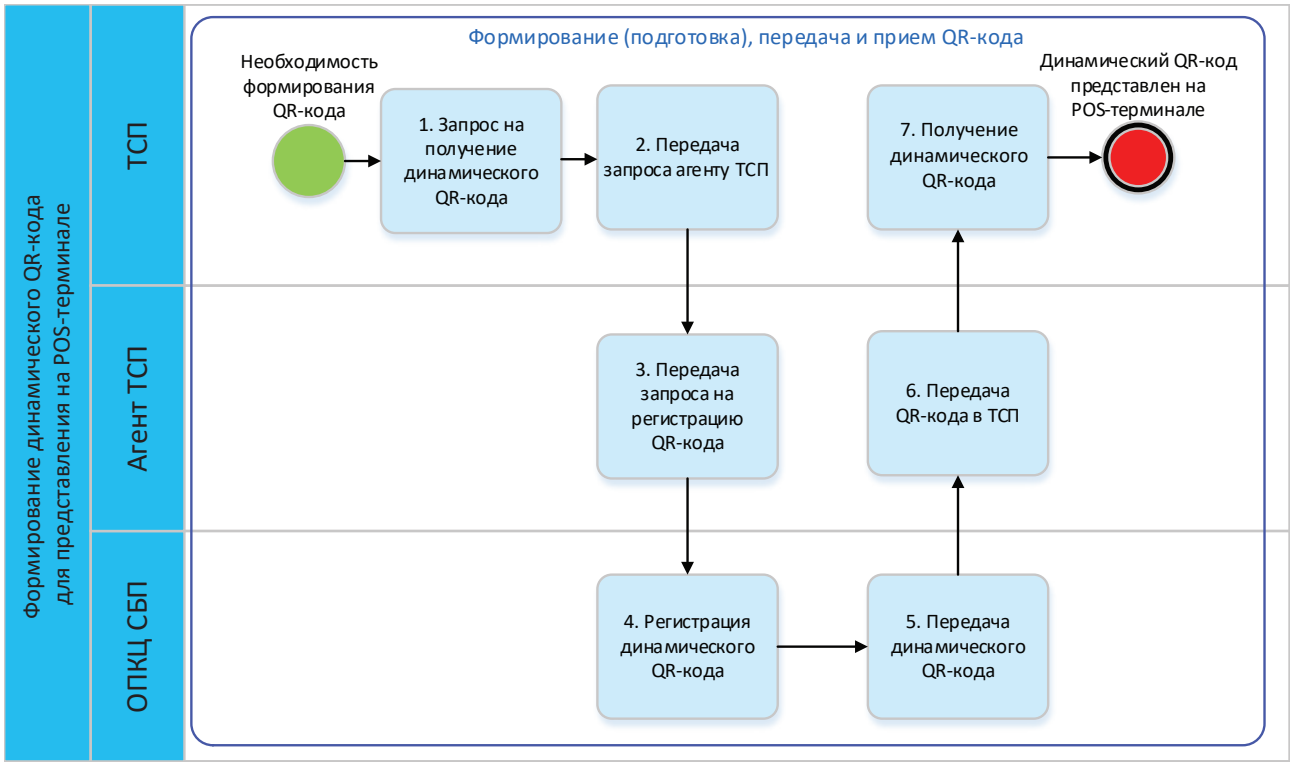
Плательщик проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика. Далее – типовой процесс C2B СБП, регламентированный в стандартах ОПКЦ СБП.

Схемы процесса представлены на рис. 47, 48. Меры защиты на технологических участках и подэтапах приведены в табл. 24.

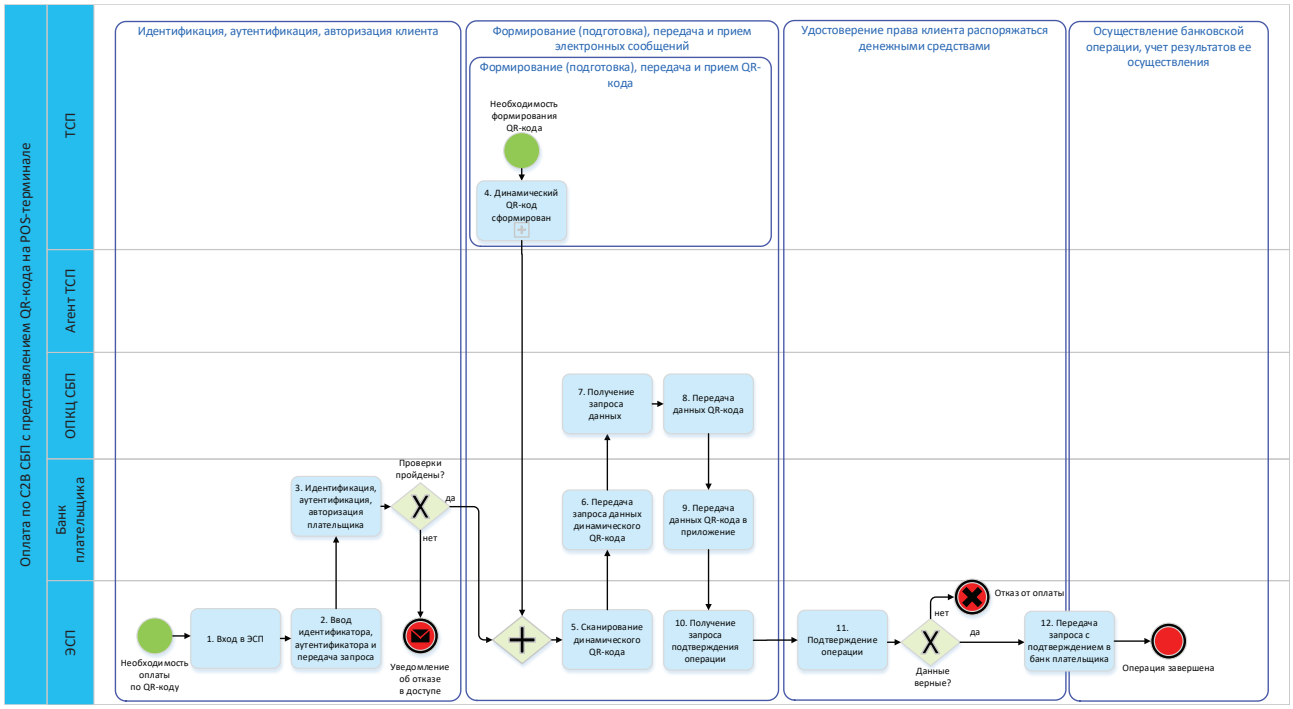
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ *Табл. 24*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.2, 3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА POS-ТЕРМИНАЛЕ *Рис. 47*



ОПЛАТА ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА POS-ТЕРМИНАЛЕ *Рис. 48*



ПРИЛОЖЕНИЕ 18. ПРОЦЕСС ОПЛАТЫ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ

Сценарий процесса

ТСП формирует и передает запрос на QR-код в статическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП (QR-код в статическом сценарии заранее сформирован).

ТСП в приложении вводит сумму платежа и передает запрос на активацию QR-кода агенту ТСП, агент ТСП передает запрос в ОПКЦ СБП. ОПКЦ СБП активирует QR-код и передает уведомление в приложение ТСП через агента ТСП. QR-код в статическом сценарии активен и представлен на мониторе ТСП / веб-браузере.

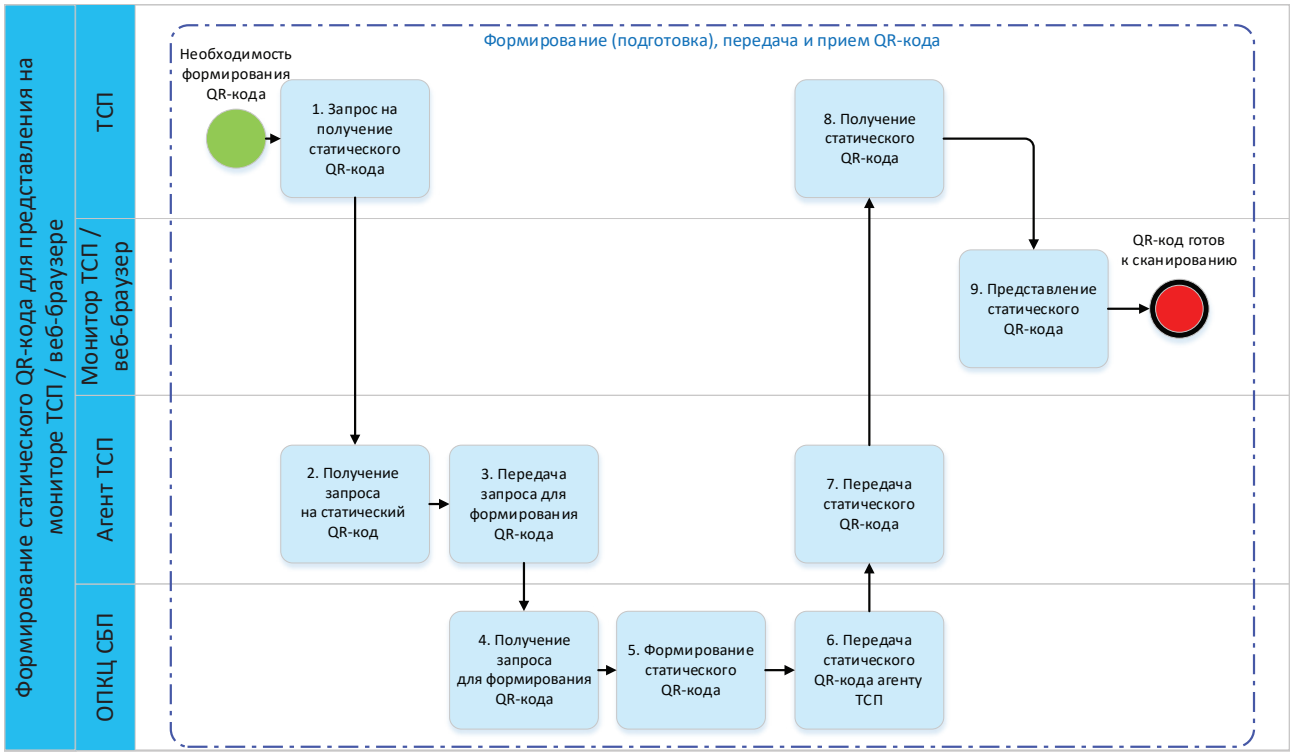
Плательщик проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика. Далее – типовой процесс C2B СБП, регламентированный в стандартах ОПКЦ СБП.

Схемы процесса представлены на рис. 49, 50. Меры защиты на технологических участках и подэтапах приведены в табл. 25.

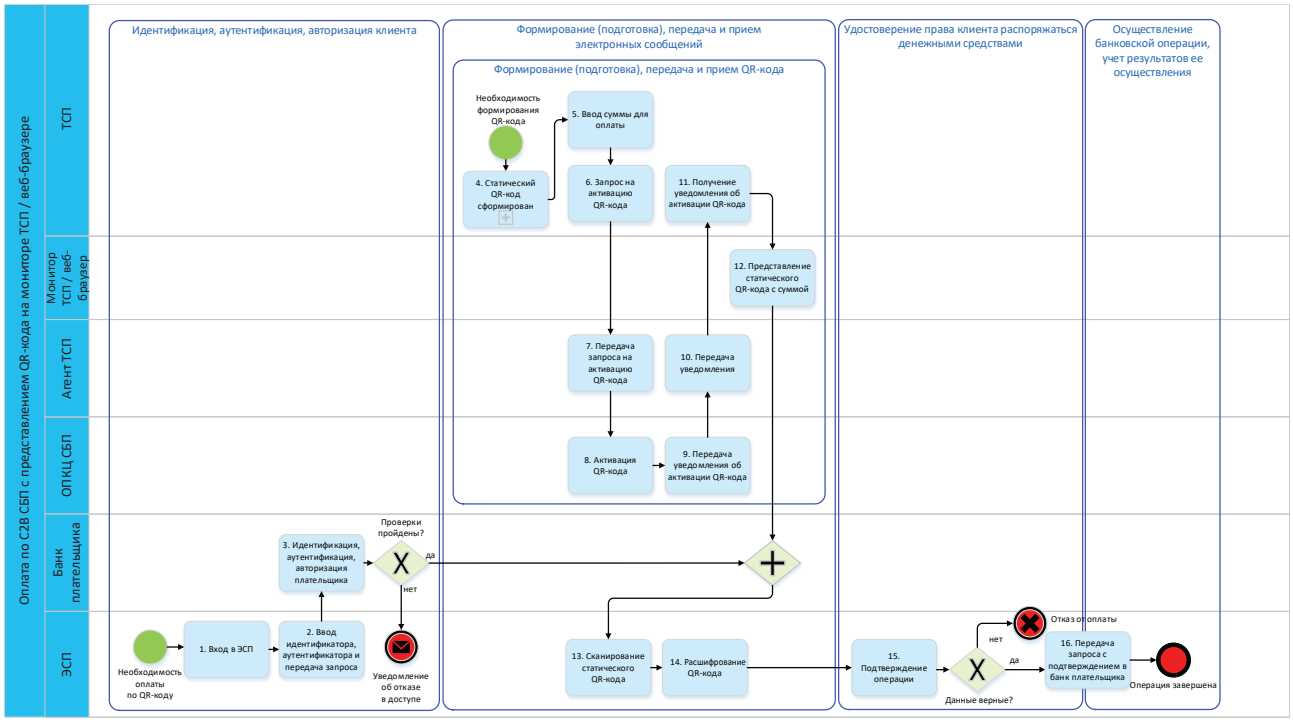
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ *Табл. 25*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2, 3.4.4
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.3.5, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.1, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1, 3.1.2, 3.1.7, 3.1.8
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ *Рис. 49*



ОПЛАТА ПО С2В СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ *Рис. 50*



ПРИЛОЖЕНИЕ 19. ПРОЦЕСС ОПЛАТЫ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ

Сценарий процесса

ТСП формирует и передает запрос на QR-код в динамическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП. QR-код в динамическом сценарии представлен на мониторе ТСП / веб-браузере.

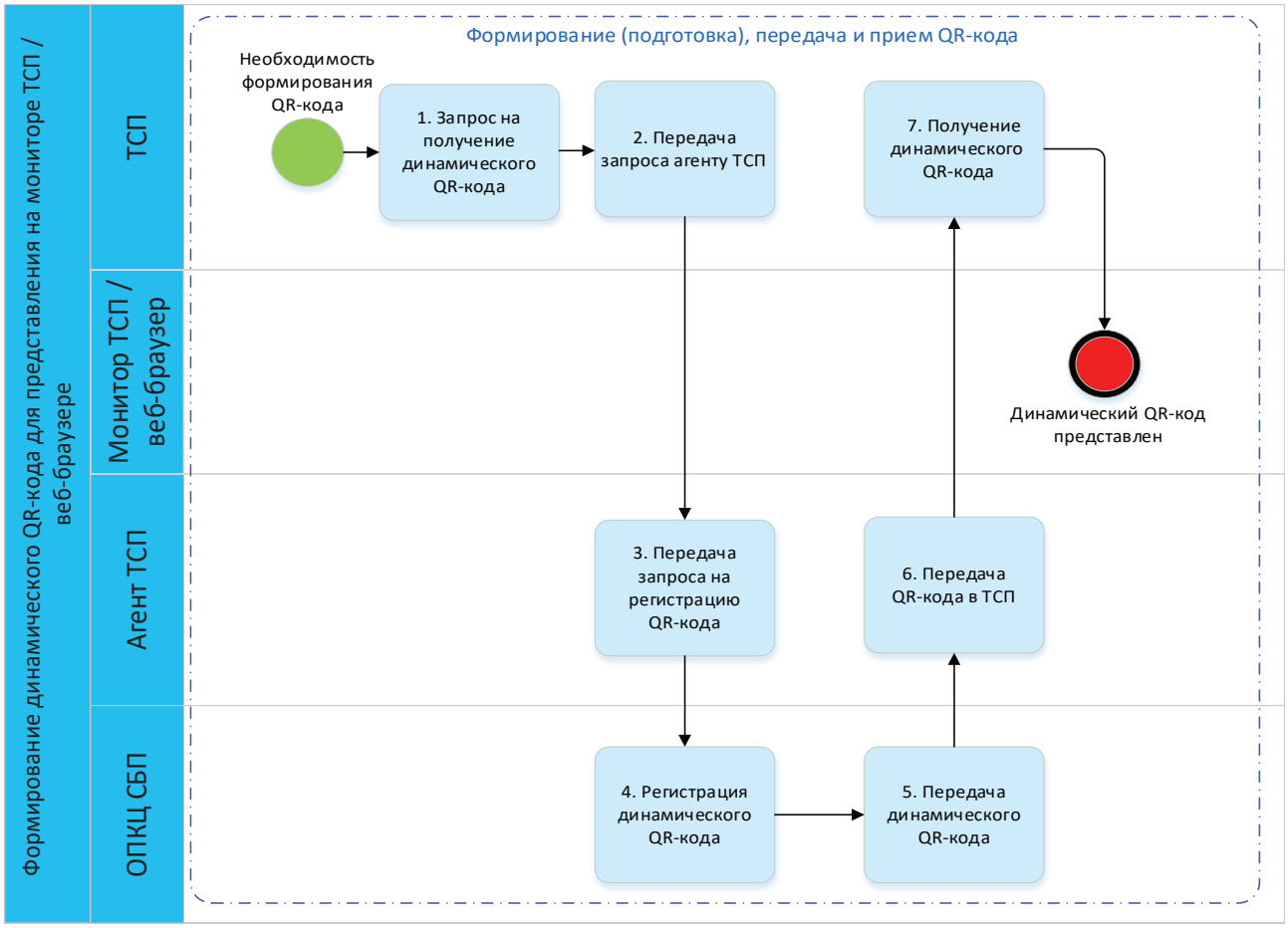
Плательщик проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика. Далее – типовой процесс C2B СБП, регламентированный в стандартах ОПКЦ СБП.

Схемы процесса представлены на рис. 51, 52. Меры защиты на технологических участках и подэтапах приведены в табл. 26.

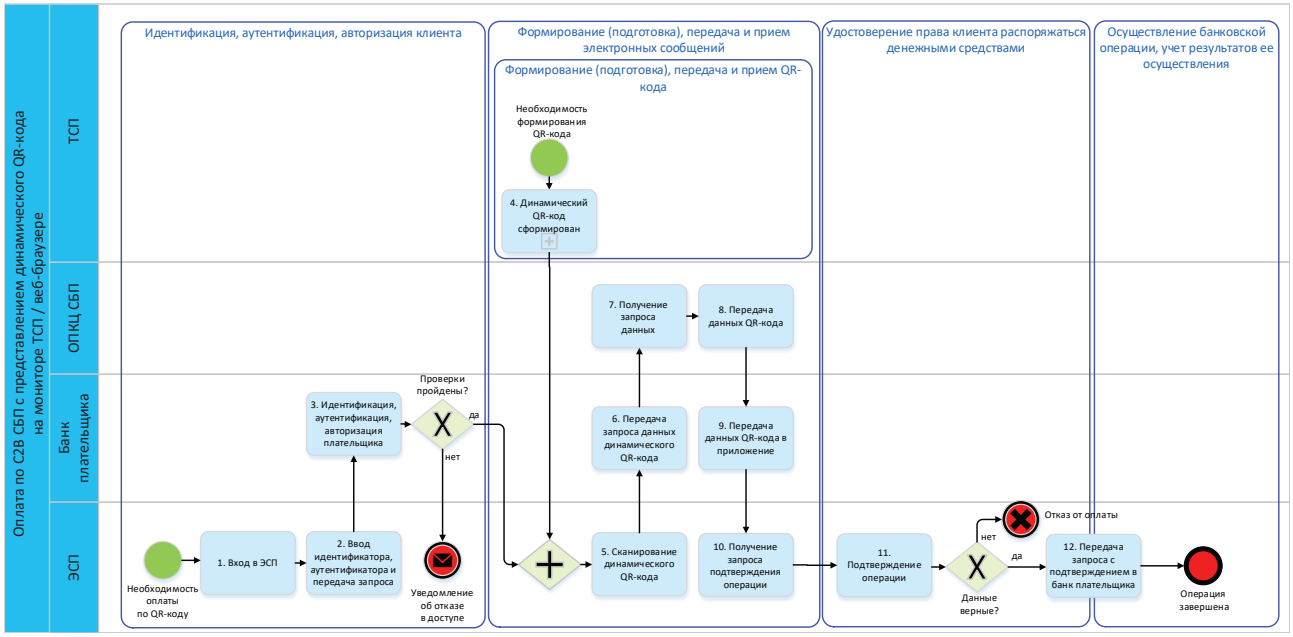
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО C2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ *Табл. 26*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ *Рис. 51*



ОПЛАТА ПО С2В СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП / ВЕБ-БРАУЗЕРЕ *Рис. 52*



ПРИЛОЖЕНИЕ 20. ПРОЦЕСС ОПЛАТЫ ПО B2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП

Сценарий процесса

ТСП формирует и передает запрос на QR-код в статическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП (QR-код в статическом сценарии заранее сформирован).

ТСП в приложении вводит сумму платежа и передает запрос на активацию QR-кода агенту ТСП, агент ТСП передает запрос в ОПКЦ СБП. ОПКЦ СБП активирует QR-код и передает уведомление в приложение ТСП через агента ТСП. QR-код в статическом сценарии активен и представлен на мониторе ТСП.

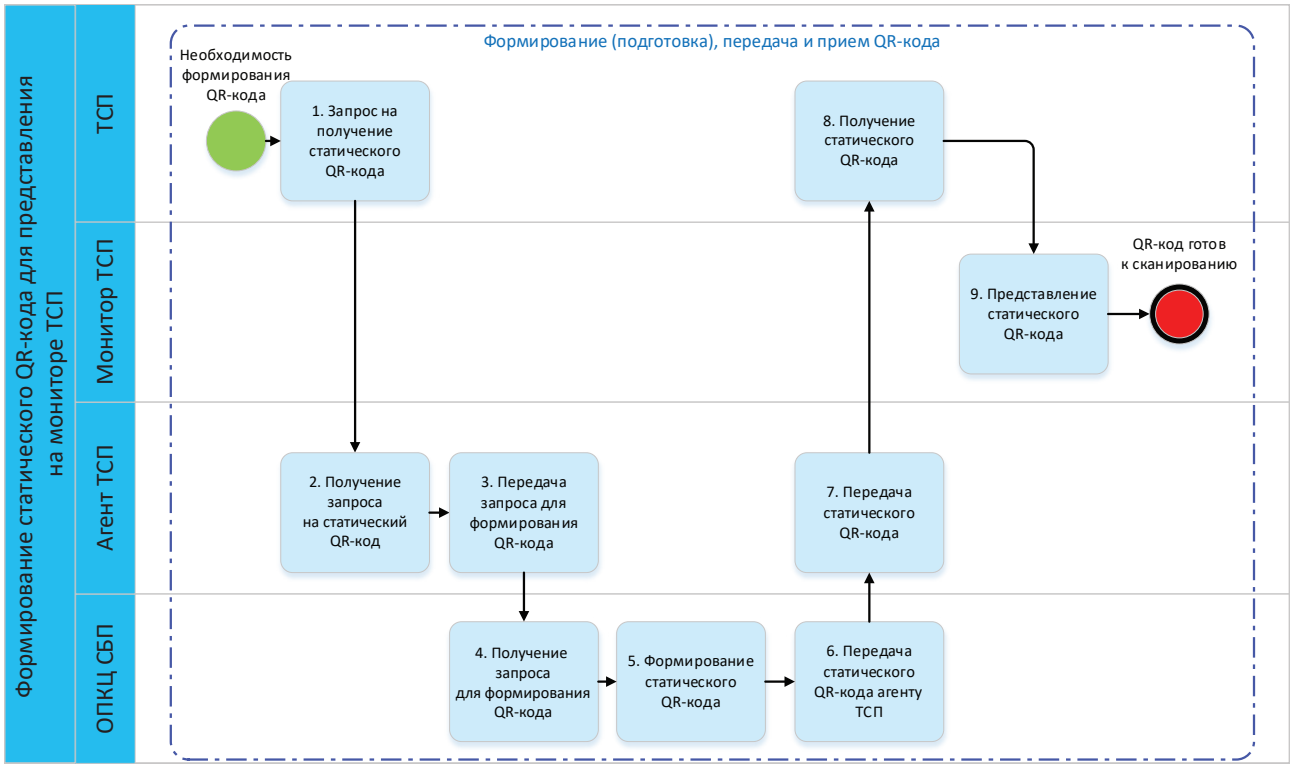
Плательщик (ЮЛ) проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика. Далее – типовой процесс B2B СБП, регламентированный в стандартах ОПКЦ СБП.

Схемы процесса представлены на рис. 53, 54. Меры защиты на технологических участках и подэтапах приведены в табл. 27.

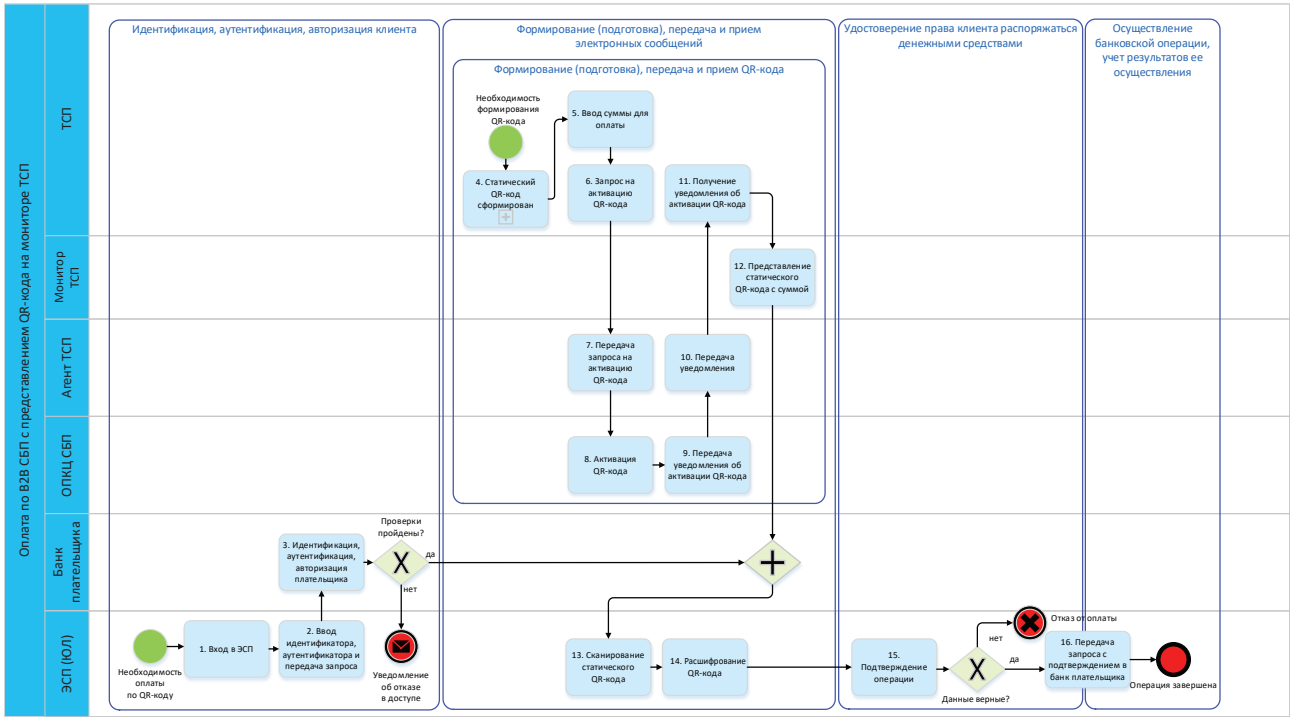
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО B2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП *Табл. 27*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2, 3.4.4
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4, 3.1.5
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1, 3.1.2, 3.1.7, 3.1.8
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.3, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ СТАТИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА МОНИТОРЕ ТСП *Рис. 53*



ОПЛАТА ПО B2B СБП С ПРЕДСТАВЛЕНИЕМ СТАТИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП *Рис. 54*



ПРИЛОЖЕНИЕ 21. ПРОЦЕСС ОПЛАТЫ ПО B2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП

Сценарий процесса

ТСП формирует и передает запрос на QR-код в динамическом сценарии агенту ТСП. Агент ТСП передает запрос на формирование QR-кода в ОПКЦ СБП. ОПКЦ СБП формирует QR-код и передает его ТСП через агента ТСП. QR-код в динамическом сценарии представлен на мониторе ТСП.

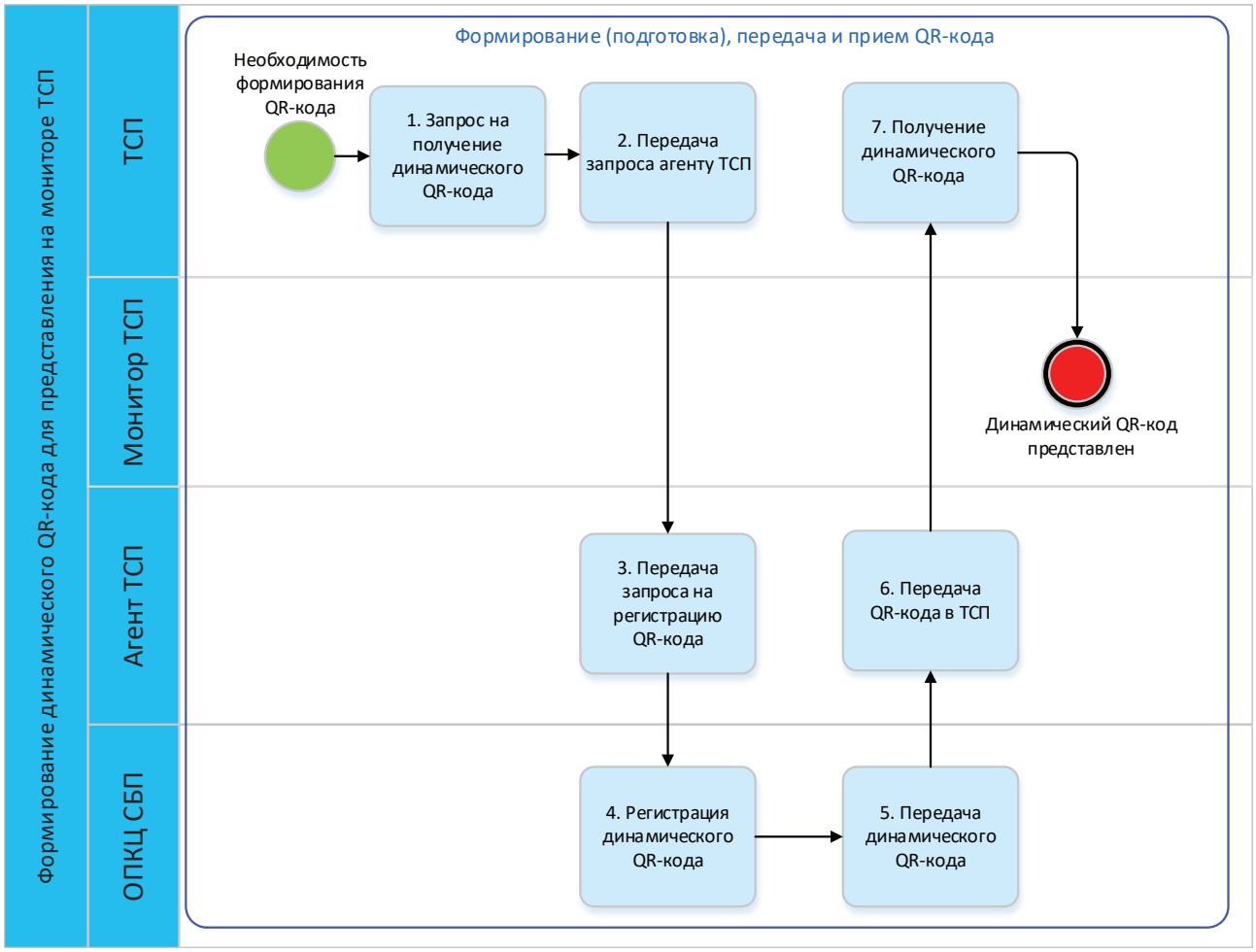
Плательщик (ЮЛ) проходит аутентификацию в ЭСП, сканирует QR-код, выбирает счет, с которого будут списаны денежные средства, проверяет реквизиты и передает запрос на перевод денежных средств в банк плательщика. Далее – типовой процесс B2B СБП, регламентированный в стандартах ОПКЦ СБП.

Схемы процесса представлены на рис. 55, 56. Меры защиты на технологических участках и подэтапах приведены в табл. 28.

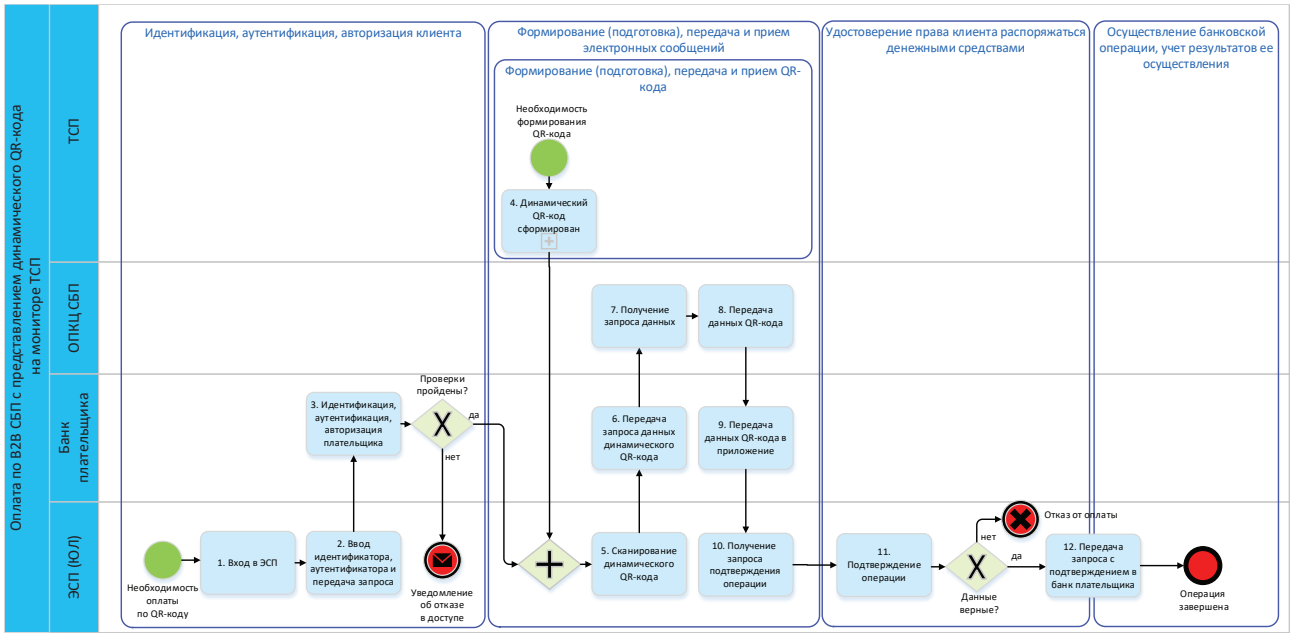
МЕРЫ ЗАЩИТЫ ПРИ ОПЛАТЕ ПО B2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП *Табл. 28*

№	Подэтап / технологический участок	Меры защиты
1.	Формирование, передача, обработка запроса (данных) для генерации QR-кода	Меры защиты из раздела 9.3: 1.1.1–1.1.3, 1.1.5, 1.2.1, 1.2.2, 1.3.1–1.3.5, 2.3.1, 2.5.1, 2.5.2, 3.4.1, 3.4.2
2.	Формирование и представление QR-кода плательщиком/получателем	1.3.6, 2.1.1, 2.3.2, 2.4.1, 2.4.3
3.	Сканирование и получение данных из QR-кода для дальнейшего осуществления перевода денежных средств	2.1.2, 2.2.3, 2.2.4, 3.2.1–3.2.3
4.	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций	1.1.4, 2.4.3
5.	Формирование (подготовка), передача и прием электронных сообщений	3.1.6
6.	Удостоверение права клиентов распоряжаться денежными средствами	2.3.4, 2.3.7, 3.1.4
7.	Осуществление банковской операции, учет результатов ее осуществления	3.1.1–3.1.3, 3.1.7, 3.1.8, 3.4.3
8.	Все шаги технологического подэтапа / технологические участки	2.2.2, 2.3.6, 2.4.2, 3.2.4

ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО QR-КОДА ДЛЯ ПРЕДСТАВЛЕНИЯ НА МОНИТОРЕ ТСП *Рис. 55*



ОПЛАТА ПО B2B СБП С ПРЕДСТАВЛЕНИЕМ ДИНАМИЧЕСКОГО QR-КОДА НА МОНИТОРЕ ТСП *Рис. 56*



СПИСОК ИСТОЧНИКОВ

1. Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

2. Положение Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

3. Стандарт ОПКЦ СБП. Термины и сокращения. П. 226. Версия 1.1.

4. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (с изменениями и дополнениями).

5. EMV® QR Code Specification for Payment Systems (EMV® QRCPS) Consumer-Presented Mode – https://www.emvco.com/specifications/emv-qr-code-specification-for-payment-systems-emv-qrcps-consumer-presented-mode/.

6. EMV® QR Code Specification for Payment Systems (EMV® QRCPS) Merchant-Presented Mode – https://www.emvco.com/specifications/emv-qr-code-specification-for-payment-systems-emv-qrcps-merchant-presented-mode/.

7. Alipay Global Portal – https://global.alipay.com/docs/.

8. ISO/DIS 20937:2023 «Financial services – Specification of QR-codes for mobile (instant) credit transfers» (www.iso.org).

9. ISO/DIS 5201:2022 «Financial services – Code-scanning payment security» (www.iso.org).

10. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 18004-2015 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода QR Code».

11. Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers EPC024-22 Version 0.6 / Date issued: 16 February 2022 – https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-02/EPC024-22v0.6%20Standardisation%20of%20QR-codes%20for%20MSCTs.pdf.