Утверждены Протоколом Правления
№ 10-11/19 от 20 марта 2025г.

Евразийский
Сберегательный Банк

Правила
пользования банковскими платежными картами в ОАО Евразийский Сберегательный Банк»

Термины и определения

Авторизация - процедура подтверждения эмитентом полномочий или авторства держателя карты на проведение им операции с использованием банковской платежной карты (транзакции), в результате которой возникает обязательство эмитента перед эквайером исполнить расчетный документ, составленный с использованием карты вышеуказанного эмитента. Авторизация может быть автоматизированной (посредством терминала) и голосовой (посредством телефонной связи). В случае, если по совершаемой с использованием банковской платежной карты операции эмитент и эквайер являются одним и тем же лицом, то авторизация является разрешением, предоставляемым эмитентом клиенту на совершение данной операции.

Банковская платежная карта (далее – карта) - платежный инструмент, используемый при проведении расчетов при покупке товаров, услуг, получении наличных денег в национальной и иностранной валютах, осуществлении денежных переводов, а также для расчетов в форме электронных денег через терминалы, банкоматы или иные устройства (периферийные устройства). Карта, оформленная по карт-счету на имя владельца карт-счета, является основной картой, а карты, оформленные по карт-счету на третьи лица, являются дополнительными картами. При истечении срока действия основной карты, а также в случае ее утраты, кражи, карта, выпускаемая взамен основной карты, также является основной картой. Карты подразделяются на дебетную и кредитную, выпущенную в виде пластиковой карты либо в электронном виде, либо токенизированную/отцифрованную версию карты, сохраненную на мобильном устройстве и позволяющую выполнять операции бесконтактной оплаты с использованием технологии NFC.

Банкомат - аппаратно-программный комплекс для выдачи и/или приема наличных денежных средств, записи денежных средств на карту, получения информации по совершенным транзакциям держателем карты, осуществления безналичных платежей и выдачи карт-чека по всем видам произведенных транзакций. Банкомат является банковским оборудованием и предназначен для самостоятельного совершения держателем операций с использованием карты без участия уполномоченного работника коммерческого банка.

Блокирование карты - полный или временный запрет на осуществление операций с использованием карты, осуществленный по инициативе держателя карты, Банка или предприятия одним из способов, установленных платежной системой. В случае полного запрета предусматривается изъятие платежной карты при ее предъявлении к обслуживанию.

Держатель карты - клиент Банка, физическое лицо, в том числе уполномоченное юридическим лицом/индивидуальным предпринимателем-владельцем карт- счета, имеющее право совершать операции с использованием карты на основании Договора с Банком, в том числе держатели основной и дополнительных карт, открытых по карт-счету, а также клиенты в рамках зарплатных проектов.

Карт-счет - банковский счет, на котором отражаются операции, осуществленные с использованием карты или ее реквизитов.

Карточная операция - операция с использованием карты и/или ее реквизитов и других

инструментов дистанционного обслуживания (например, покупка товаров, услуг, перевод денежных средств, обмен валют или получение наличных денежных средств), в результате которой происходит изменение остатка денежных средств на карт-счете держателя карты.

Call Centre – подразделение Банка, являющееся круглосуточным контактным центром, предназначенным для обработки дистанционных обращений существующих и потенциальных клиентов Банка. Телефоны Call Centre:(312) 905151

Мобильное устройство - это любое портативное устройство держателя карты, на котором установлен Платежный мобильный сервис и имеется поддержка технологии NFC (например, смарт-часы, смартфон, планшет и т.п.).

Мультипликатор - коэффициент в виде процентной надбавки к сумме авторизации по карточной операции, применяемый Банком в целях нивелирования риска возникновения задолженности по карт-счету в случае осуществления карточной операции в валюте, отличной от валюты ведения карт- счета. Проведение окончательных взаиморасчётов по карточной операции (списание суммы карточной операции с карт-счета держателя карты) производится без применения мультипликатора. Виды карточных операций, по которым применяется мультипликатор, определяются Баком самостоятельно. Размер мультипликатора устанавливается Банком в зависимости от рыночной конъюнктуры на валютным рынке и может быть изменен Банком в одностороннем порядке. Информация о размере мультипликатора указывается на корпоративном сайте Банка www.esb.kg.

Платежная система расчетов с использованием банковских платежных карт (далее платежная система) – система расчетов с использованием карт, эмитируемых и обслуживаемых в соответствии с требованиями операторов данных систем и законодательством Кыргызской Республики. Платежной системой устанавливаются определенные правила осуществления взаимных расчетов по платежам с использованием карт между участниками системы. Платежные системы подразделяются на локальные (национальную) (Элкарт) и международные (Visa, Mastercard).

Платежный мобильный сервис – программное обеспечение Провайдера, предоставляемое держателю карты на основании отдельного соглашения (договора), заключенного между провайдером и держателем карты, представляющее собой приложение, установленное на мобильном устройстве, позволяющее токенизировать карты, удалить токен, использовать токен для осуществления операций. Функциональные возможности Платежного мобильного сервиса, условия его использования и порядок предоставления держателю карты прав на его использование определяются Провайдером. В случае если Банк выступает в качестве Провайдера, Платежным мобильным сервисом является Мобильное приложение Банка. К таким платёжным мобильным сервисам относятся системы мобильных платежей по средствам электронных кошельков (Google Pay, Garmin Pay и др.), которые в сочетании с программным обеспечением на мобильном устройстве, обладающем технологией NFC, предоставляют возможность оплачивать покупки и снимать денежные средства.

Постирование (или клиринг) - процесс сбора, обработки, подтверждения платежей и подсчета взаимных обязательств участников платёжной системы за осуществлённые карточные операции, осуществляемые путём взаимного зачёта, исходя из условий баланса платежей и представляют собой окончательный финансовый взаиморасчет по карточной операции.

Процессинг – лицензируемая деятельность, включающая в себя взаимосвязанные процессы по приему, обработке и выдаче участникам платежной системы финансовой информации.

Процессинговый центр (далее - ПЦ) – юридическое лицо, осуществляющее процессинг.

Провайдер – юридическое лицо, являющееся производителем (разработчиком) Платежного мобильного сервиса, которое обеспечивает на основании правил платежных систем и/или на основании отдельного соглашения с платежной системой информационное и технологическое взаимодействие при формировании, обслуживании и использовании токена в целях проведения карточной операций. Кроме того, провайдером может являться Банк, при использовании держателем карты программного обеспечения Банка;

Рекуррентные платежи - регулярные карточные операции (платежи), проводимые в сети Интернет либо карточные операции (платежи), производимые посредством дистанционного банковского обслуживания по ранее сохраненным реквизитам карты, не требующие участия и подтверждения со стороны держателя карты (например, абонентская оплата / оплата по подписке за услуги интернет-ресурсов, оплаты товаров или услуг в рассрочку, регулярные «авто платежи»).

Социальная инженерия - это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют мошенникам получить защищаемую/секретную информацию держателя карты, с целю хищения денежных средств.

Стоп-лист - список заблокированных карт, по которым приостановлено или временно приостановлено совершение всех и/или определенных видов операций.

Токенизация карты — это технология, предоставляемая платежными системами и предназначенная для обмена конфиденциальных данных карты на специальный обезличенный эквивалент (токен), для защиты реквизитов карты. В процессе токенизации создается связка реквизитов карты и токена, позволяющая однозначно определить карту, использованную для совершения операций с использованием токена. Операции, совершенные с использованием токена, равнозначны операциям, совершенным держателем карты с использованием самой карты или ее реквизитов.

Токен – цифровое представление карты, которое формируется по факту токенизации карты и хранится в зашифрованном виде в защищенном облачном хранилище платежной системы, а также сохраняется в памяти мобильного устройства.

Фишинг (phishing от fishing «рыбная ловля, выуживание») - один из видов интернет-мошенничества, целью которого является получение доступа к секретной и защищаемой информации держателя карты - реквизитам и паролям карт, и/или логину и паролю от систем дистанционного банковского обслуживания. Чаще всего мошенники входят в доверие держателя карты и заполучают карточные реквизиты и пароли посредствам социальных сетей, мессенджеров. В основном используется метод проведения массовых рассылок, в том числе от имени банка или крупных и известных компаний, которые могут содержать ссылки на ложные сайты, внешне неотличимые от настоящих. В подобных рассылках или сообщениях держателя карты зачастую попросят обновить или подтвердить верность персональной информации, путем отсылки на поддельный сайт, где держатель карты добровольно вводит свои учетные данные / реквизиты карты. В случае, если мошенникам удается получить данную информацию, это приводит к краже денежных средств с карт-счета. Ответственность за подобного рода операции несет держатель карты.

Эквайер - Банк, получивший разрешение на осуществление эквайринга, владелец сети периферийных устройств, обеспечивающий возможность проведения авторизации или транзакций через свои периферийные устройства в соответствии с технологией и нормативными актами соответствующих платежных систем и законодательством Кыргызской Республики

Эквайринговая сеть - включает в себя все устройства банков-эквайеров участников платежных систем, которые предназначены для осуществления карточных операций: банкоматы; кассовые POS-терминалы, установленные в отделениях банков; торговые POS-терминалы, установленные в торгово- сервисных предприятиях; платежные терминалы; автоматические депозитные машины; электронная коммерция.

Электронная коммерция (E-commerce) - деятельность торгово-сервисных предприятий, имеющих договорные отношения с эквайером на предмет осуществления финансовых/торговых безналичных карточных операций, осуществляемые через интернет-сайты с использованием компьютерных сетей.

Эмбоссированное имя держателя карты - фамилия и имя держателя карты в латинской транскрипции, отпечатанные на лицевой стороне карты.

Эмитент - Банк, осуществляющий выпуск карт в соответствии с технологией и правилами соответствующих платежных систем и законодательством Кыргызской Республики.

CVV2-код (Card verification value) - трехзначный код для проверки подлинности карты,

запрашиваемый при оплате через Интернет и иных операциях.

Near Field Communication (NFC) – технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, и/или картой и устройствами. По требованию большинства платежных систем карты должны поддерживать технологию бесконтактной оплаты **(NFC).**

PIN-код (Personal identification number, далее - ПИН-код) - персональный идентификационный номер, позволяющий аутентифицировать пользователя для совершения операции. ПИН-код является паролем доступа к карте и относится к секретной и защищаемой информации, и не подлежащей разглашению третьим лицам, отличным от держателя карты. ПИН-код карты присваивается с целью идентификации личности ее держателя при проведении карточных операций.

POS-терминал (point-of-sale) - терминал для приема оплаты за товары и услуги в торгово-сервисных предприятиях с использованием карты и других инструментов дистанционного обслуживания.

3D Secure пароль - защищенный протокол, который используется как дополнительный уровень безопасности для двухфакторной аутентификации пользователя по транзакциям без присутствия карты. Технология была разработана для платежной системы Visa с целью улучшения безопасности интернет-платежей в рамках услуги Verified by Visa (VbV). Услуги, основанные на данном протоколе, также были приняты платежными системами Mastercard под названием Mastercard SecureCode (MSC). 3D Secure пароль формируется динамически и предназначен для использования при совершении покупок в сети Интернет.

QR-код - двухмерный символ штрих кода для передачи платежных данных, который используется при проведении безналичных платежей и переводов.

Глава 1. Общие положения

1.1. Правила пользования банковскими платежными картами ОАО "Евразийский Сберегательный Банк" (далее по тексту – Правила) определяют условия пользования, условия обслуживания и меры безопасности при совершении карточных операций по картам платежных систем, эмитируемых ОАО "Евразийский Сберегательный Банк" (далее по тексту — Банк).

1.2. Настоящие Правила составлены в соответствии с Положением Национального банка Кыргызской Республики «О банковских платежных картах в Кыргызской Республике».

1.3. Настоящие правила являются стандартными (типовым) и не подлежат изменению со стороны держателя карты. Банк может пересмотреть настоящие Правила в одностороннем порядке по мере необходимости, разместив информацию о внесенных изменениях на корпоративном сайте www.esb.kg в разделе «Новости» с учетом срока, установленного действующим законодательством Кыргызской Республики для информирования о предстоящих изменениях.

Глава 2. Порядок выдачи и хранения карты

2.1. Банк выдает карту непосредственно держателю карты, либо доверенному лицу, действующему на основании нотариально удостоверенной доверенности. В случае согласия держателя карты, карта может быть направлена ему посредством курьерской организации, в этом случае держатель карты должен подтвердить факт получения карты путем предоставления затребованных Банком данных (фото/видео подтверждения или иные сведения, которые Банк потребует от держателя карты).

2.1.1. Выдача держателям карт в рамках зарплатных проектов, осуществляется путем передачи Банком карт уполномоченному представителю организации, на основании нотариально удостоверенной доверенности или за подписью руководителя или иного лица, уполномоченного на это учредительными документами, с приложением печати этой организации.

2.2. Передача карты третьим лицам, не являющимися держателем карты, в пользование или в качестве залога запрещается.

2.3. На лицевой стороне карты содержатся:

2.3.1. логотип Банка;
2.3.2. логотип платежной системы;
2.3.3. встроенный чип - интегральная микросхема с закодированной на ней информацией;
2.3.4. номер карты, состоящий из 16 цифр;
2.3.5. эмбоссированное имя клиента (фамилия и имя держателя карты на латинице или инициалы, если фамилия и имя клиента превышает 22 латинских знака);
2.3.6. дата истечения срока действия карты;

2.4. На оборотной стороне карты содержатся:
2.4.1. магнитная полоса
2.4.2. место для подписи клиента (опционально);
2.4.3. номер Call Centre Банка;
2.4.4. проверочный код (CVV2);

2.5. Держателю карты необходимо предохранять карту от механических повреждений и от воздействия электромагнитных полей (автомобильные сигнализации, мобильные телефоны, компьютеры, пропускные рамки в аэропортах, банках, магазинах и т. п.) во избежание повреждений магнитной полосы.

2.6. Запрещено оказывать любое физическое воздействие каким-либо предметом на поверхность ПИН-конверта, чипа или карты в целом. В случае повреждения карты, чипа или ПИН-конверта в результате намеренных, халатных или непреднамеренных действий держателя карты, карта перевыпускается за счет держателя карты согласно действующим Тарифам Банка.

2.7. Размер комиссий и тарифов за выпуск и обслуживание карт, а также расходных и приходных лимитов карточных операций, лимитов по операциям перевода денежных средств, лимитов на конвертацию денежных средств в разрезе валюты и/или типа банковского счета, лимитов по бесконтактным платежам, разрешенных для проведения без введения ПИН-кода, определяется Тарифами Банка. Информация о размерах лимитов, комиссий и тарифов размещена на корпоративном сайте Банка www.esb.kg.

2.8. В целях безопасности Банк не рекомендует устанавливать сверхбольшие размеры по суммам лимитов на длительный период времени. Ответственность за последствия несоблюдения настоящего пункта возлагается на держателя карты.

2.9. Карт-счет предназначен только для совершения следующих карточных операций:
2.9.1. зачисления/списания с/на карт-счет физических лиц денежных средств в наличном и безналичном порядке некоммерческого характера;
2.9.2. зачисления на карт-счет юридических лиц денежных средств в наличном и безналичном порядке коммерческого характера;
2.9.3. списания с карт-счета физических и юридических лиц денежных средств в счет оплаты товаров, услуг торгово-сервисных предприятий и иных третьих лиц;
2.9.4. списания с карт-счета держателя карты денежных средств в оплату комиссий Банка и задолженности по кредиту/кредитам (включая технический овердрафт);
2.9.5. списания с карт-счета физических и юридических лиц денежных средств в погашение задолженности перед Банком, возникшей в процессе выпуска и обслуживания платежной карты, в том числе сверх остатка денежных средств на карт-счете, либо возникшей по другим обстоятельствам в силу иных договоров между Банком и держателем карты;
2.9.6. зачисления и списания с карт-счета физических и юридических лиц денежных средств в сумме переводных операций (включая комиссии Банка согласно действующих Тарифов);
2.9.7. списания с карт-счета физических и юридических лиц денежных средств на основании исполнительных документов, предусмотренных действующим законодательством Кыргызской Республики.

2.10. Банк вправе предоставить держателю карты возможность осуществить токенизацию для дальнейшего совершения карточных операций с использованием токена (мобильного устройства, на котором хранится токен).

2.11. По инициативе держателя карты, карта может быть подвязана к платежным мобильным сервисам (электронным кошелькам) для оплаты и снятия денежных средств с

использованием технологии токенизации и оплаты посредством мобильного устройства с использованием модуля NFC. При этом при совершении операции с использованием токена, верификация держателя карты осуществляется путем ввода держателя карты пароля в Мобильном устройстве и, в случае необходимости, дополнительным вводом ПИН-кода (при платежах через POS-терминал или Банкомат).

2.12. В целях обеспечения возможности совершения карточных операций с использованием технологии бесконтактных платежей (NFC), в том числе с целью предоставления Держателю карты в мобильном приложении Банка информации о совершенных им карточных операциях, Банк имеет право передавать информацию о сумме карточной операции, дате и времени ее совершения, типе операции, коде валюты, статусе авторизации для ее обработки Провайдерам (Google Ireland Limited, Garmin Ltd. и т.д.) программного обеспечения платежных мобильных сервисов (Google Pay, Garmin Pay и т.п.).

2.13. При использовании Держателем карты технологии NFC, Банк не несет ответственности:

2.13.1. за последствия, которые могут возникнуть в случае, если информация о токенизированной карте, в том числе о балансе такой карты, отображаемая на экране устройства, станет известна третьим лицам;

2.13.2. за ситуации, связанные со сбоями в работе систем, обеспечивающих прием, обработку и передачу данных по операциям, совершенным с использованием карты по независящим от Банка причинам, за работу сервиса Google Pay, Garmin Pay.

2.14. Осуществление Держателем карты карточных операций с использованием платежных мобильных сервисов (Google Pay, Garmin Pay и т.п.) может быть ограничено функциональностью программного обеспечения мобильного устройства Держателя карты, в том числе мобильного приложения Банка.

2.15. Держатель карты осознает повышенный риск и понимает, что при использовании платежных мобильных сервисов (Google Pay, Garmin Pay и т.п.) доступ к мобильному устройству Держателя напрямую влияет на возможность несанкционированных операций по карте, а, следовательно, Держатель карты самостоятельно несет ответственность за конфиденциальность одноразовых паролей, паролей, ПИН, и других средств доступа Держателя карты к мобильному устройству, мобильному приложению, карте.

2.16. Токен может быть удален Держателем карты самостоятельно на мобильном устройстве или через обращение в Банк. Блокировка Токена производится через обращение в Банк.

Глава 3. ПИН-код

3.1. Карта выдается держателю карты вместе со специальным конвертом, где напечатан ПИН-код, (либо посредством отправки SMS-уведомления/PUSH-уведомления на номер мобильного телефона, указанного в заявлении Клиента при открытии счета). Держателю карты рекомендуется сразу при получении карты вскрыть конверт, убедиться в том, что ПИН-код напечатан разборчиво, запомнить ПИН-код (SMS-уведомление/PUSH-уведомление) и далее хранить конверт раздельно от карты и в недоступным для третьих лиц месте.

3.2. ПИН-код неизвестен работникам Банка и должен сохраняться держателем карты в секрете в течении всего времени пользования картой.

3.3. Утерянный ПИН-код на бумажном носителе, либо в SMS-уведомлении/PUSH-уведомлении не восстанавливается, а карта подлежит перевыпуску согласно Тарифам Банка.

3.4. Рекомендуется придерживаться определенных правил для обеспечения секретности ПИН-кода:

3.4.1. запрещено записывать ПИН-код на карте;

3.4.2. запрещено хранить ПИН-конверт с ПИН-кодом и карту рядом (в одном месте);

3.4.3. не позволяйте третьим лицам подсматривать набираемые на клавиатуре устройства (банкомат, терминал) цифры ПИН-кода;

3.4.4. не допускайте ошибок при наборе цифр ПИН-кода. При неправильном наборе

ПИН-кода (три раза подряд) лимит попыток набора ПИН-кода заканчивается, карта автоматически блокируется и дальнейшее проведение карточной операции невозможно. В таком случае держателю карты рекомендуется обратиться в ближайшее отделение Банка или в Call Centre Банка для обнуления попыток неверного ввода ПИН-кода.

3.5. Карточные операции, подтверждаемые набором ПИН-кода, считаются Банком совершенными держателем карты и не подлежат оспариванию по причине несанкционированного доступа к карт-счету и/или мошенничества

Глава 4. Пользование картой в торгово-сервисных предприятиях

4.1. Безналичная оплата товаров, услуг и работ в торгово-сервисных предприятиях (далее - ТСП) производится в пределах установленного лимита по карте и лимита в эквайринговом устройстве банка-эквайера.

4.2. Максимальный размер одной операции и количество операций в сутки в эквайринговом устройстве Банка и/или стороннего банка-эквайера определяется Тарифами Банка, политикой банка-эквайера и правилами платежных систем.

4.3. Оплата товаров и услуг может быть проведена посредством:

- 4.3.1. считывания магнитной ленты карты и ввода ПИН-кода;
- 4.3.2. считывания магнитной ленты карты без ввода ПИН-кода;
- 4.3.3. считывания чипа карты и ввода ПИН-кода;
- 4.3.4. считывания чипа карты без ввода ПИН-кода;
- 4.3.5. считывания бесконтактного чипа через бесконтактный чип-ридер без ввода ПИН-кода в пределах установленных лимитов согласно Тарифам Банка, банка-эквайера и/или правил платежных систем;
- 4.3.6. считывания бесконтактного чипа через бесконтактный чип-ридер с вводом ПИН-кода для сумм свыше установленного лимита согласно Тарифам Банка, банка-эквайера и/или правил платежных систем;
- 4.3.7. использования токена карты без ввода ПИН-кода (в пределах установленных лимитов) или с вводом ПИН-кода (для сумм свыше установленного лимита). Лимиты регулируются политикой Банка, банка - эквайера и/или правилами платежных систем;
- 4.3.8. считывания QR-кода для проведения денежного перевода или безналичного платежа за товары или услуги ТСП.

4.4. Безналичная оплата товаров и услуг в ТСП может производиться либо в режиме онлайн, либо в режиме офлайн, в зависимости от установленных настроек устройств банка-эквайера. Ответственность за проведение операций в режиме офлайн лежит на держателе карты. При этом оплата товаров и услуг в POS - терминалах, принадлежащих Банку, в режиме офлайн по умолчанию запрещена.

4.5. Оплата товаров и услуг, а также снятие денежных средств с ошибкой считывания чипа в устройствах, поддерживающих чиповую технологию, запрещена (Fallback транзакции).

4.6. Карты Банка выпускаются с возможностью проведения бесконтактных платежей (PayWave / NFC), которая не может быть отключена по инициативе держателя карты в связи с требованием платежных систем об обязательной поддержке технологии бесконтактной оплаты.

4.7. Все транзакции с использованием карты в ТСП должны проводиться в присутствии держателя карты. Это необходимо в целях снижения риска неправомерного получения персональных данных держателя карты, указанных на карте. В некоторых ТСП может быть запрошен документ удостоверяющий личность. Поэтому при оплате покупки картой, Банк рекомендует иметь при себе паспорт или иной удостоверяющий личность документ.

4.8. Все ТСП оснащаются указателями с логотипами платежных систем для информирования держателей карт о возможности обслуживания той или иной карты в данном ТСП, а также о возможности приема платежей с использованием QR-кода.

4.9. Для проведения карточных операций держателю карты необходимо вставить / приложить карту или поднести мобильное устройство, в случае токенизации карты, к устройству (банкомат, платежный терминал, POS-терминал) или отсканировать QR-код

через мобильное приложение Банка при оплате посредством QR-кода.

4.10. Для проведения карточных операций через ТСП или Банк, сотрудник ТСП или Банка осуществляет авторизацию с помощью POS-терминала. Карта помещается или прикладывается в считывающее устройство POS-терминала.

4.11. Предварительно сотрудником ТСП или Банка вводится сумма карточной операции на клавиатуре POS-терминала. В некоторых случаях, например, при превышении лимита суммы карточной операции, разрешенной к проведению без ПИН-кода, может быть запрошен у держателя карты ПИН-код, который необходимо ввести на специальной клавиатуре. При наборе правильного ПИН-кода и достаточности денежных средств на карт-счете распечатывается чек в двух экземплярах, подтверждающий успешное завершение карточной операции. При использовании технологии бесконтактных платежей или токенизированной карты Держатель карты должен поднести карту или мобильное устройство на минимальное расстояние к POS-терминалу или Банкомату для совершения карточной операции или отсканировать QR-код через мобильное приложение Банка при оплате посредством QR-кода.

4.12. Держателю карты рекомендуется:

4.12.1. удостовериться в корректности данных, указанных в чеке;

4.12.2. забрать один экземпляр чека POS-терминала до момента полного взаиморасчета по данной карточной операции, а также в целях сверки расходных операций по карт-счету.

4.13. Для операций, подтвержденных ПИН-кодом, а также бесконтактных операций, проведенных без введения ПИН-кода в пределах установленного лимита подпись держателя карты на чеке не обязательна.

4.14. Требования по подписи чека при проведении операций в эквайринговой сети стороннего эквайера определяется политикой данного эквайера.

4.15. Держателю карты запрещается подписывать чек торгового POS-терминала, в котором не указана сумма покупки (товара/услуги).

4.16. По правилам платежных систем ТСП не вправе завышать стоимость товаров и услуг при принятии карты к оплате по сравнению с наличным расчетом. При выявлении таких случаев, держателю карты рекомендуется уведомить Банк.

4.17. Возврат оплаченной по карте покупки или услуги производится с согласия ТСП. Для этого по обращению держателя карты сотрудником ТСП должна быть инициирована на POS-терминале операция «возврат покупки». Возврат суммы покупки наличными денежными средствами не предусматривается.

Глава 5. Пользование картой в банкомате

5.1. Как правило, наличные денежные средства выдаются по карте в валюте страны пребывания. Некоторые банки-эквайеры могут установить дополнительную комиссию за выдачу наличных денежных средств. Также в некоторых странах частота и максимальная сумма выдачи наличных денежных средств по карте могут ограничиваться законодательством.

5.2. Перед использованием банкомата необходимо осмотреть его на наличие нехарактерных ему устройств: неровно установленной ПИН-клавиатуры, накладок в картоприемнике, наличие мини-видеокамер, направленных на ПИН-клавиатуру, накладок над экраном банкомата и иных подозрительных устройств. Если держатель карты обнаружил наличие нехарактерных устройств рекомендуется не использовать данный банкомат и сообщить в Call Centre банка-эквайера по номерам, указанным на банкомате.

5.3. Для получения денежных средств или иных услуг в банкомате необходимо вставить карту в картоприемник банкомата или поднести мобильное устройство в случае токенизации карты, ввести ПИН-код, выбрать соответствующее меню и следовать инструкциям на экране.

5.4. Для того, чтобы отказаться от услуги, необходимо отменить операцию нажатием кнопки «Отмена» / «Cancel».

5.5. При работе с банкоматом, не допускается применение физической силы для того, чтобы вставить карту в банкомат. Если карта не вставляется, необходимо воздержаться от использования такого банкомата.

5.6. При введении ПИН-кода необходимо убедиться, чтобы ПИН-код не видели третьи лица. После 3 (трех) попыток ввода неправильного ПИН-кода карта блокируется и может быть задержана (изъята) банкоматом.

5.7. После появления на экране команды «ЗАБЕРИТЕ СВОЮ КАРТУ» - необходимо незамедлительно забрать карту, в противном случае через 15-30 секунд карта может быть задержана банкоматом.

5.8. После появления на экране команды «ЗАБЕРИТЕ СВОИ ДЕНЬГИ» - необходимо незамедлительно забрать денежные средства, в противном случае через 20 секунд денежные средства будут задержаны банкоматом.

5.9. Рекомендуется всегда забирать чек о проведенной операции через банкомат, поскольку чек является документом, подтверждающим совершение карточной операции в случае разрешения спорных ситуаций. В виду наличия в чеке информации, относящейся к держателю карты, рекомендуется чек забирать с собой и не оставлять его возле банкомата.

5.10. Причинами неуспешных карточных операций по карте в банкомате могут быть следующие:

5.10.1. запрашиваемая сумма в данный момент не может быть выдана банкнотами, имеющимися в кассетах банкомата. В такой ситуации рекомендуется запрашивать сумму, кратную минимальному номиналу банкнот, указываемому в инструкции (экранном меню) к данному банкомату;

5.10.2. запрашиваемая сумма превышает лимит разовой выдачи, определяемый техническими характеристиками банкомата. В такой ситуации рекомендуется разделить запрашиваемую сумму на части и повторить операцию несколько раз;

5.10.3. запрашиваемая сумма превышает доступный баланс карт-счета (с учетом комиссии Банка и/или банка-эквайера). В такой ситуации рекомендуется запросить меньшую сумму. Доступный баланс карт-счета может быть уточнён в том числе путем запроса через меню банкомата операции доступного остатка денежных средств по карте.

5.11. В случае изъятия карты банкоматом, необходимо убедиться, что карта действительно задержана (банкомат продолжает обслуживать других клиентов или перестал функционировать). В противном случае, банкомат может вернуть карту другому клиенту и/ или выдать ему запрошенные денежные средства.

5.12. В случае изъятия карты банкоматом держателю карты рекомендуется незамедлительно заблокировать карту любым удобным способом: через обращение в Call Centre Банка или самостоятельно через мобильное приложение Банка. В дальнейшем Банк рекомендует выпустить новую карту с новыми реквизитами, т.к. при изъятии карты существует риск доступа третьих лиц к карте и/или реквизитам карты.

5.13. Если карта или денежные средства оказались задержанными банкоматом, необходимо незамедлительно связаться с Банком или банком-эквайером по телефонам, указанным на банкомате.

Глава 6. Пользование картой в сети Интернет

6.1. Карточные операции в сети Интернет производится в пределах установленного лимита на Интернет платежи и лимита банка-эквайера.

6.2. Оплата за товары или услуги в сети Интернет производится без физического присутствия карты, но с использованием реквизитов карты, обязательными из которых являются: номер карты, срок действия карты, эмбоссированное имя держателя карты. Дополнительно при проведении платежей в сети Интернет могут быть запрошены такие реквизиты карты, как: CVV2, 3D Secure пароль в соответствии с условиями

обслуживания Интернет-ресурса. Оплата за товары или услуги в сети Интернет также может быть осуществлена с использованием токена.

6.3. Банк выпускает карты с доступом к Интернет-платежам «по умолчанию».

6.4. Держатель карты может закрыть доступ к проведению Интернет-платежей (за исключением карточных операций, осуществляемых с введением 3D Secure пароля, и рекуррентных платежей). Для этого держателю карты рекомендуется обратиться в Банк с письменным заявлением на отключение доступа к Интернет- платежам или самостоятельно отключить доступ через мобильный банкинг «ЕСБ».

6.5. Карты VISA и Mastercard Банка подключены к сервису 3D Secure «по умолчанию». Протокол 3D Secure не применяется для операций, проводимых посредством карт Элкарт.

6.6. Оплата за товары и услуги на Интернет-ресурсах, поддерживающих технологию 3D Secure и требующих ввода 3D Secure пароля, без ввода 3D Secure пароля запрещены (ECI 06).

6.7. Карточные операции в сети Интернет могут быть проведены следующими способами:

6.7.1. посредством использования токена или указания реквизитов карты, обязательными из которых являются: эмбоссированное имя держателя карты, номер карты, срок действия карты, дополнительно может быть запрошен CVV2 код, а также 3D Secure пароль, на Интернет сайтах поддерживающих данную технологию;

6.7.2. посредством привязки реквизитов карты или токена к Интернет-аккаунту, электронному кошельку, магазину, торговой площадке, интернет-сервису или иным ресурсам в сети Интернет согласно требованиям и условиям обслуживания Интернет-ресурса. В случае привязки карты / токена становится возможным проведение рекуррентных платежей. Ответственность по такого рода операциям несет держатель карты до момента отвязки реквизитов карты / дезактивации токена. При этом держателю карты рекомендуется сохранить свидетельства об отвязке карты или дезактивации токена от рекуррентных платежей, которые могут потребоваться в случае возникновения спорных моментов у держателя карты с интернет- ресурсом.

6.8. Доступ на проведение транзакций в сети Интернет свыше лимита, установленного тарифами Банка, производится:

6.8.1. путем обращения держателя карты в отделение Банка и подачи письменного заявления на изменение действующих лимитов и ограничений на Интернет-платежи.

6.9. Перед совершением операции в сети Интернет Банк рекомендует держателю карты:

6.9.1. проверить срок действия карты и отсутствие блокировки карты;

6.9.2. убедиться в достаточности денежных средств на карте;

6.9.3. убедиться в наличии открытого доступа по карте к Интернет-платежам и достаточности лимитов для данного рода карточных операций;

6.9.4. убедиться в наличии установки на своём браузере обновлений безопасности;

6.9.5. совершать Интернет-платежи только на проверенных сайтах с положительной репутацией, а также сайтах, поддерживающих технологию безопасных Интернет-платежей (3D Secure);

6.9.6. Воздержаться от совершения операций на автоматически перенаправленных страницах или всплывающих окнах во избежание «Фишинга». В большинстве случаев «Фишинга», мошеннический клон-сайт, на который может быть настроена переадресация, выглядит идентично настоящему и может лишь незначительно отличатся от оригинального сайта, например, частью URL-адреса;

6.9.7. Для отмены Интернет-платежа, полной или частичной, держателю карты в первую очередь необходимо обратиться в службу поддержки клиентов Интернет-магазина для инициирования возврата платежа.

6.10. При бронировании услуг в сети Интернет по категории Travel & Entertainment

(«Путешествие и Развлечение», таких как: аренда автомобиля, гостиницы, покупка билетов и т.д.) Банк вправе заблокировать деньги на карт- счете держателя карты до завершения полного расчета с ТСП. При этом банк-эквайер имеет право на увеличение суммы окончательного списания в размере, предусмотренном правилами соответствующей платежной системы. Держатель карты несет полную ответственность по оплате добавленной стоимости по карточным операциям, относящимся к категории Travel & Entertainment.

Глава 7. Меры безопасности при обращении с картой

7.1. Номер карты, ПИН-код, CVV2 код, срок действия карты, эмбоссированное имя держателя карты, код клиента в Банке (client ID), 3D Secure и OTP пароли, а также логин и пароль от банка — представляют собой реквизиты карты и секретную информацию, которые обеспечивают доступ к денежным средствам держателя карты, поэтому относятся к категории защищаемой информации, не подлежащей рассекречиванию и передаче третьим лицам.

7.2. Держатель карты несет ответственность за сохранность реквизитов карты и секретной информации. Реквизиты карты и секретная информация не должны быть известны третьим лицам. Держатель карты обязан хранить реквизиты карты и секретную информацию в безопасном и недоступном для третьих лиц месте.

7.3. Использование карты, реквизитов карты, секретной информации (ПИН- код, 3D Secure и OTP пароли, логин и пароль от мобильного приложения Банка), а также использование мобильного устройства, содержащим данные о токенизированной карте, третьими лицами не допускается.

7.4. Держатель карты несет ответственность за соблюдение и за последствия при несоблюдении пунктов 7.8-7.10 настоящих Правил. Держатель карты соглашается, что при выявлении случаев нарушения пунктов 7.8-7.10 настоящих Правил ведет к блокированию карты Банком в одностороннем порядке.

7.5. Держателю карты запрещено:

7.5.1. записывать какие-либо данные из реквизитов карты, а также пароль/логин мобильного банкинга «ЕСБ» или пароли мобильного устройства на самой карте или хранить их вместе или рядом с картой;

7.5.2. оставлять карту и/или ее реквизиты, а также мобильное устройство или иную секретную информацию в местах, доступных для копирования и/или записи и/или использования третьими лицами;

7.5.3. передавать третьими лицам реквизиты карты (все или часть), одноразовые пароли, а также пароль/логин от мобильного приложения Банка, пароли от мобильного устройства.

7.6. Вся финансовая и материальная ответственность за карточные операции, совершенные по карте и/или ее реквизитам, в том числе с использованием или без использования паролей карты (ПИН-код, 3D Secure пароль), а также за операции, совершенные в мобильном банкинге «ЕСБ» (в том числе операции, проведенные посредством считывания QR-кода) или с использованием мобильного устройства (в том числе токенизированные операции) третьими лицами, возлагается на держателя карты.

7.7. В случае утери, кражи или подозрений на использование карты или ее реквизитов третьим лицом, и/или получения держателем карты смс/push-уведомления с информацией о карточной операции, которую он не совершал, а также в случае добровольной передачи мобильного устройства или секретной информации третьим лицам, или при утере/краже мобильного устройства и/или компрометации токена, держатель карты обязан НЕЗАМЕДЛИТЕЛЬНО обратиться в Банк по официальным каналам связи, размещенным на корпоративном сайте Банка www.esb.kg, для блокировки карты / токена, или заблокировать карту самостоятельно посредством мобильного банкинга «ЕСБ», выбрав соответствующую причину блокировки, когда данный факт стал известен держателю карты или у держателя карты возникли подозрения по данному факту. Держатель карты несёт ответственность за все карточные операции и свои действия или бездействия и/или действия или бездействия

третьих лиц до момента блокировки карты / мобильного банкинга «ЕСБ»

7.8. Утерянная/украденная карта или карта со скомпрометированными реквизитами или секретной информацией подлежат блокировке и не подлежит перевыпуску, пролонгации с сохранением основных карточных реквизитов. Держателю карты необходимо обратиться в Банк для выпуска новой карты с новыми реквизитами карты. Дальнейшее использование и/или разблокировка утерянных/украденных/скомпрометированных карт запрещены.

7.9. В случае, если утерянная/украденная/скомпрометированная карта была разблокирована по инициативе держателя карты, вся ответственность за возможные последующие несанкционированные списания по карте лежит на держателе карты. Держатель карты теряет право на инициирование диспутного процесса согласно правилам платежных систем.

7.10. Клиент обязан соблюдать следующие требования по безопасности в целях исключения несанкционированных операций с использованием токена:

7.10.1. не оставлять мобильное устройство без присмотра;

7.10.2. обеспечить надлежащий уровень безопасности на мобильном устройстве, используя пароли и другие возможные способы блокировки/разблокировки мобильного устройства;

7.10.3. убедиться в том, что на мобильном устройстве не зарегистрированы отпечатки пальцев или иные способы аутентификации другого лица, включая распознавание лица;

7.10.4. не разглашать третьим лицам пароль от мобильного устройства;

7.10.5. удалить все личные данные и финансовую информацию с мобильного устройства, если прекращено его использование;

7.10.6. незамедлительно обратиться в Банк по номеру телефона, предусмотренному на оборотной стороне карты, либо по официальным каналам связи, размещенным на корпоративном сайте Банка www.esb.kg, в случае подозрений на любое несанкционированное использование токена, а также, если мобильное устройство было взломано, утеряно или украдено;

7.10.7. не блокировать любые функции безопасности, предусмотренные на мобильном устройстве в целях защиты токена;

7.10.8. в обязательном порядке создать сложный пароль и сохранять только свои биометрические данные (отпечатки пальца, распознавание лица и другие) для использования мобильного устройства;

7.10.9. удалить все личные данные и финансовую информацию с мобильного устройства при передаче мобильного устройства третьим лицам или временно заблокировать через обращение в Банк;

7.10.10. не подвергать мобильное устройство операциям повышения привилегий/взлома операционной системы устройства (jail break, rooting и другие);

7.10.11. не использовать платежный мобильный сервис при подключении к беспроводным сетям общего доступа;

7.10.12. не производить верификацию в платежный мобильный сервис на мобильном (-ых) устройстве (-ах), принадлежащего (-их) третьему (-им) лицу (-ам).

7.11. Держатель карты несёт полную ответственность за любые убытки, возникшие в результате совершения карточных операций в рамках «Дружеского фрода» и/или в результате «Фишинга» и/или «Социальной инженерии».

7.12. В целях отслеживания операций по карт-счету и своевременного реагирования и блокирования карты в случае несанкционированного доступа к карт-счету, держателю карты рекомендуется подключить услугу получения смс/push-уведомлений по карточным операциям.

7.13. Держателю карты рекомендовано не менее 1 (одного) раза в месяц контролировать состояние карт-счета. Для этих целей держатель карты может самостоятельно формировать выписку в мобильном банкинге, либо обратиться в Банк за получением выписки по карт-счету.

Глава 8. Обработка карточных операций

8.1. Карточная операция в рамках правил платежных систем обрабатывается в два этапа:

8.1.1. **Авторизация** - 1 этап, предусматривающий блокировку денежных средств на карт-счете держателя карты; на этапе авторизации доступный баланс карт-счета уменьшается на сумму успешно авторизованной расходной карточной операции.

8.1.2. **Постирование** - 2 этап, предусматривающий принятие карточной операции к учету, которое осуществляется после получения всех документов по данной карточной операции. На данном этапе происходит окончательная финансовая обработка карточной операции, т.е. списание или зачисление денежных средств по карт-счету держателя карты в зависимости от типа карточной операции (расходная или приходная).

8.2. На период между датой авторизации и постированием карточной операции сумма карточной операции (с учтём комиссий) блокируется на карт-счете держателя карты и окончательно постируется в период до 33 (Тридцати трех) календарных дней.

8.3. Блокирование денежных средств по успешным карточным операциям на этапе авторизации приводит к уменьшению или увеличению доступного баланса карт-счета в зависимости от характера карточной операции: расходная или приходная. Расходная карточная операция всегда приводит к уменьшению доступного баланса, а приходная карточная операция увеличивает доступный баланс карт-счета в случае, если это предусмотрено правилами платежных систем.

8.4. Постирование операций производится после получения Банком электронного финансового документа от банка-эквайера через соответствующую платежную систему.

8.5. В случае отсутствия постирования операций от банка-эквайера по истечению срока, указанного в п.8.2. настоящих Правил, сумма денежных средств по успешной карточной операции автоматически выходит из блока (разблокируется) и становится доступной держателю карты для повторного использования.

8.6. В случае получения Банком позднего списания (постирование операций в срок свыше 33 календарных дней) от банка-эквайера, Банк вправе произвести безакцептное списание с карт-счета держателя карты денежных средств в размере ранее разблокированных сумм успешных карточных операций.

8.7. На этапе авторизации при блокировании суммы на карт-счете по успешным карточным операциям, проведенным в валюте отличной от валюты ведения карт-счета, Банком может быть применен мультипликатор. Постирование карточных операций выполняется без применения мультипликатора.

8.8. Обработка карточных операций:

8.8.1. при проведении карточной операции в эквайринговой сети Банка в валюте, отличной от валюты карт-счета, обработка карточной операции производится по коммерческому курсу Банка, установленному на день проведения авторизации.

8.8.2. при проведении карточной операции в эквайринговой сети стороннего Банка в валюте, отличной от валюты карт-счета, обработка карточной операции производится в EUR по курсу платежной системы на дату авторизации карточной операции.

8.8.3. в случае возникновения технического овердрафта по карт-счету, данная задолженность учитывается по курсу Межбанковской платежной системой (МПС), действующему на момент образования данной задолженности.

8.9. При проведении карточных операций в валюте, отличной от валюты карт- счета, Банк производит конвертацию денежных средств в валюту карт-счета без акцепта в соответствии с Главой 12 настоящих Правил. Настоящим держатель карты уполномочивает Банк на проведение такого безакцептного конвертирования денежных средств по карт-счету на основании настоящих Правил и Договора и без какого-либо дополнительного согласия в любой форме со стороны держателя карты.

8.10. Полный возврат ранее списанной с карт-счета суммы карточной операции,

производится по инициативе банка-эквайера/ТСП в полной сумме и валюте первоначальной карточной операции. В случае если валюта карточного счета отлична от валюты карточной операции, полная отмена карточной операции производится по коммерческому курсу Банка, установленному на дату первоначальной карточной операции.

8.11. Частичная отмена карточной операции производится по инициативе банка-эквайера/ТСП в частичной сумме и валюте первоначальной карточной операции.

8.12. В случае поступления денежных средств на карту в виде кредитной карточной операций (credit и/или credit adjustment и т.п.) и/или возвратной карточной операции (reversal), которая приводит к увеличению доступного баланса карт-счета держателя карты (далее кредитная/возвратная карточная операция), Банк имеет право в одностороннем порядке заблокировать карточный счет и/или карту на срок до 30 (Тридцати) календарных дней в случае отсутствия у держателя карты документов, подтверждающих обоснованность кредитных/возвратных карточных операций. В случае образования технического овердрафта по карт-счете в результате отзыва банком-эквайером суммы ранее поступившей кредитной и/или возвратной карточной операции, держатель карты обязан погасить образовавшуюся задолженность по карт-счету по первому требованию Банка.

Глава 9. Урегулирование споров по карточным операциям

9.1. В случае наличия у держателя карты спорных карточных операций (финансовой претензии), держателю карты рекомендовано обратиться в Банк для подачи заявления установленного образца на проведение расследования (Заявление о диспутной операции (далее-«Заявление на опротестование транзакции по карте/устройству Банка»), а также, в случае необходимости, предоставить документы, подтверждающие право держателя карты на возврат денежных средств по спорной карточной операции.

9.2. В случае обоснованности претензии держателя карты, Банк от имени держателя карты в рамках правил платежных систем инициирует финансовую претензию в сторону банка-эквайера.

9.3. В случае согласия банка-эквайера с финансовой претензией держателя карты, Банк восстанавливает сумму карточной операции на карт-счете в порядке и сроки, установленных правилами соответствующих платежных систем и внутренними процедурами Банка.

9.4. За необоснованные финансовые претензии платежными системами установлены штрафные комиссии, которые могут превышать сумму спорной карточной операции. Банк вправе без согласия держателя карты списать с карт- счета штрафные комиссии и сумму необоснованной финансовой претензии.

9.5. Не подлежат оспариванию по причине мошенничества или несанкционированного доступа к карт-счету и признаются совершенными держателем карты следующие карточные операции:

9.5.1. карточные операции, совершенные с введением ПИН-кода, прошедшие с физическим предъявлением карты, при которых прошло считывание данных чипа карты и/или магнитной полосы;

9.5.2. карточные операции, совершенные без введения ПИН-кода, по контактным / бесконтактным (PayWave) платежам прошедшие с физическим предъявлением карты;

9.5.3. карточные операции, проведенные с вводом 3D Secure пароля;

9.5.4. карточные операции, совершенные в мобильном банкинге «ЕСБ», в том числе операции по QR-коду;

9.5.5. карточные операции, совершенные по токену карты.

9.6. Карточная операция считается санкционированной держателем карты, если в течении 120 (ста двадцати) календарных дней с даты ее совершения, держателем карты не было подано «Заявление на опротестование транзакции по карте/устройству Банка» в Банк по причине несанкционированного доступа к карт-счету.

9.7. Банк имеет право отказать в принятии «Заявления на опротестование транзакции по карте/устройству Банка» в случае если срок обращения держателя карты превысил 120

(сто двадцать) календарных дней с даты оспариваемой карточной операции.

9.8. В целях контроля за проводимыми карточными операциями по карт-счету и своевременного реагирования и блокирования карты в случае несанкционированного доступа к карт-счету, держателю карты рекомендуется подключить услугу получения смс/push-уведомлений по карточным операциям, а также регулярно самостоятельно формировать в мобильном приложении Банка или запрашивать в отделениях Банка выписку по карт-счету.

Глава 10. Мониторинг карточных операций и блокировка карт

10.1. Банк проводит мониторинг карточных операций с целью выявления подозрительных, мошеннических и/или нехарактерных карточных операций, с целью уменьшения риска несанкционированного доступа к карт-счетам держателей карт Банка.

10.2. Банк может заблокировать карту по результатам мониторинга с целью уточнения участия держателя карты в проведении карточной операции, а также:

10.2.1. при подозрении на мошенничество со стороны держателя карты или участие держателя карты в мошеннической схеме;

10.2.2. при подозрении о проведении операций, подпадающих под финансирование террористической деятельности, финансирование распространения оружия массового уничтожения и легализации («отмывания») преступных незаконных доходов, а также при подозрении о включении держателя карты в санкционные перечни государственной службы финансовой разведки, и в перечень лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов.

10.3. в случае наличия негативных отзывов пользователей социальных сетей или участников групп в адрес держателя карты. Блокирование карты/карт-счета осуществляется Банком в одностороннем порядке, при этом блокирование по причинам, указанным в п. 10.2. настоящих Правил, может быть осуществлено на срок до 30 (тридцать) календарных дней с правом Банка на дальнейшее продление срока блокирования до выяснения всех обстоятельств.

10.4. В случае выявления Банком множественных неуспешных авторизаций по карте: 5 (пять) и более неуспешных карточных операций в течении 2 (двух) календарных дней, по рекуррентным платежам по причине закрытых доступов и/или недостаточности денежных средств и/или отсутствия связи с держателем карты для уточнения участия в карточной операции и/или отсутствия пополнения карт-счета и/или отписки/отвязки карты от рекуррентных платежей, Банк имеет право поместить карту в стоп-лист.

Глава 11. Инструкция по оплате с помощью QR-кода и правила безопасности

11.1. Инструкция по оплате с помощью QR-кода:

11.1.1. Шаг 1: Откройте мобильное приложение банка.

11.1.2. Шаг 2: Найдите функцию по оплате с помощью QR-кода в главном меню мобильного приложения Банка.

11.1.3. Шаг 3: Направьте камеру смартфона на QR-код, который вам предоставили. Убедитесь, что QR-код полностью виден в поле для сканирования.

11.1.4. Шаг 4: После сканирования убедитесь, что информация о платеже (сумма, получатель) совпадает с указанной. Проверьте все детали платежа / перевода внимательно.

11.1.5. Шаг 5: Подтвердите оплату / перевод. Введите необходимые данные, если требуется (например, сумму), и подтвердите платеж. Возможно, потребуется ввести PIN-код или воспользоваться биометрической аутентификацией (отпечаток пальца, лицо).

11.1.6. Шаг 6: Убедитесь, что вы получили уведомление о успешной оплате. Сохраните или сделайте скриншот подтверждения для своей безопасности.

11.2. Правила безопасности при осуществлении оплаты / перевода с помощью QR-кода:

11.2.1. регулярно обновляйте мобильное приложение банка до последней версии для защиты от уязвимостей и угроз безопасности.

11.2.2. включите уведомления о транзакциях в приложении банка, чтобы следить за всеми операциями на вашем счете.

11.2.3. осуществляйте покупки / переводы только через официальное мобильное приложение банка, скачанное из проверенных источников (Google Play, App Store).

11.2.4. перед оплатой / переводом убедитесь в подлинности сканируемого QR кода, для исключения риска подмены QR кода (например, убедитесь в отсутствии переклейки статического QR-кода в торговой точке).

11.2.5. если для оплаты / перевода при считывании QR-кода, вы перенаправляетесь на сайт убедитесь, что URL начинается с «https://» и принадлежит официальному домену. Не вводите свои личные данные или данные банковской карты, в том числе секретную информацию по карте или мобильного приложения на непроверенных или подозрительных сайтах.

11.2.6. При ошибочном переводе, если вы перевели / оплатили неправильную сумму через QR-код, сообщите об этом продавцу, добросовестный торговец незамедлительно должен осуществить возврат лишних денег. Вся ответственность за платежи / переводы денежных средств, совершенные по QR-коду, возлагаются на держателя карты. Переводы денежных средств, в том числе осуществленные с помощью QR-кода, считаются добровольными и безотзывными.

Глава 12. Конвертация денежных средств

12.1. В дату проведения расчетов с МПС сумма совершенной операции по карте списывается со счета карты и зачисляется платежной системой на счет ТСП.

12.2. **Списание по операции (оплата товаров и услуг) картой Visa:**

Валюта карты	**Валюта транзакции**		
	KGS	*EUR*	*Другие валюты*
KGS	Без конверсии	Сумма операции в валюте, отличающейся от KGS, конвертируется МПС Visa в KGS по внутреннему курсу МПС **на дату проведения списания** со счета карты	
EUR	Сумма операции в KGS конвертируется в EUR по курсу Банка **на дату проведения списания** со счета карты	Без конверсии	Сумма операции в валюте, отличающейся от EUR и KGS, конвертируется МПС Visa в EUR по внутреннему курсу МПС **на дату проведения списания** со счета карты

12.3. **Списание по операции (оплата товаров и услуг) картой Mastercard:**

Валюта карты	**Валюта транзакции**			
	KGS	*EUR*	*USD*	*Другие валюты*

KGS	Без конверсии	Сумма операции в валюте, отличающейся от KGS, конвертируется МПС Mastercard в KGS по внутреннему курсу МПС на дату проведения списания со счета карты		
EUR	Сумма операции в KGS конвертируется в EUR по курсу Банка **на дату проведения списания** со счета карты	Без конверсии	Сумма операции в валюте, отличающейся от KGS и EUR, конвертируется МПС Mastercard в EUR по внутреннему курсу МПС **на дату проведения списания** со счета карты	
USD	Сумма операции в KGS конвертируется в USD по курсу Банка **на дату проведения списания** со счета карты	Сумма операции в валюте EUR, конвертируется МПС Mastercard в USD по внутреннему курсу МПС **на дату проведения списания** со счета карты	Без конверсии	Сумма операции в валюте, отличающейся от KGS и USD, конвертируется МПС Mastercard в USD по внутреннему курсу МПС **на дату проведения списания** со счета карты