УТВЕРЖДЕНО
Протокол правления
ОАО «Белагропромбанк»
20.06.2013 № 41
(в редакции протокола
Правления
ОАО «Белагропромбанк»
29.07.2025 № 68)

ПРАВИЛА ПОЛЬЗОВАНИЯ БАНКОВСКИМИ ПЛАТЕЖНЫМИ КАРТОЧКАМИ (ДАЛЕЕ – ПРАВИЛА)

Настоящие правила пользования банковскими платежными карточками (далее - Правила) являются частью договора текущего (расчетного) банковского счета, доступ к которому обеспечивается посредством использования банковской платежной карточки, договора текущего (расчетного) банковского счета физического лица с базовыми условиями обслуживания, и (или) иных платежных инструментов (далее - Договоры), заключенного между ОАО «Белагропромбанк» (далее - Банк) и физическим лицом (далее - Клиент), определяют для Банка и Клиента права, обязанности, иные условия и размещаются на официальном сайте Банка в глобальной компьютерной сети Интернет по адресу: www.belapb.by.

1. Средства с текущего (расчетного) банковского счета, доступ к которому обеспечивается посредством использования банковской платежной карточки, текущего (расчетного) банковского счета физического лица с базовыми условиями обслуживания и (или) иных платежных инструментов (далее – счет), используются для расчетов по операциям, совершенным при использовании всех банковских платежных карточек (далее – карточки) (либо их реквизитов), выпущенных в рамках Договора, в том числе для оплаты вознаграждения Банку.

2. При ведении счета в иностранной валюте:

если погашение задолженности по Договору осуществляется путем внесения Клиентом наличной иностранной валюты в кассу Банка и часть средств, необходимых к погашению, составляет менее минимального номинала банкноты соответствующей иностранной валюты, то Клиент вносит сумму иностранной валюты, превышающую часть средств, необходимых к погашению, а Банк покупает у Клиента разницу между минимальным номиналом банкноты соответствующей иностранной валюты и частью средств к погашению по обменному курсу покупки наличной иностранной валюты, установленному в момент совершения операции в Подразделении Банка, в котором осуществляется операция;

если при закрытии счета в иностранной валюте часть средств, необходимых к выдаче Клиенту, составляет менее минимального номинала банкноты соответствующей иностранной валюты, то Банк покупает у Клиента часть средств менее минимального номинала банкноты соответствующей иностранной валюты по обменному курсу наличной иностранной валюты, установленному в момент совершения операции Подразделением Банка, в

котором осуществляется операция.

При этом валютно-обменные операции оформляются в соответствии с законодательством и ЛПА, регламентирующим порядок осуществления валютно-обменных операций с участием физических лиц.

3. Счет может быть пополнен другим физическим лицом (далее – иное физическое лицо) с соблюдением требований законодательства.

4. Банк имеет право устанавливать для Клиента поощрение в виде Money-back (доход, выплачиваемый Банком в виде процента от суммы безналичной оплаты товаров, работ и услуг) или иные виды поощрений при расчетах карточкой в рамках программ лояльности и премиальных программ.

Банк имеет право предоставлять Клиенту дополнительные сервисы и услуги по отдельным видам карточек («консьерж-сервис», Premium Card и др.).

В случае отмены/возврата безналичной операции оплаты товаров, работ и услуг, совершенной с выплатой поощрения в виде Money-back, Банк имеет право списать со счета Клиента ранее зачисленную сумму дохода.

Правила программ лояльности и премиальных программ публикуются Банком на официальном сайте Банка в глобальной компьютерной сети Интернет по адресу www.belapb.by. Внесение изменений (дополнений) в Правила программ лояльности и премиальных программ, приостановление действия, закрытие программ лояльности и премиальных программ осуществляется Банком в одностороннем порядке.

5. Клиент поручает Банку списывать с его Счета платежным ордером Банка 0,3 % от суммы каждой безналичной операции, совершенной с использованием карточки, выпущенной в рамках благотворительного проекта «Прикосновения», и (или) ее реквизитов, и ежеквартально перечислять указанную сумму в местный благотворительный фонд «Прикосновение к жизни».

В целях исполнения части первой настоящего пункта к безналичным операциям относятся операции по оплате товаров, работ и услуг в ОТС, операции без предъявления благотворительной карточки, а именно операции по оплате товаров, работ и услуг через глобальную компьютерную сеть Интернет. Не относятся к безналичным операциям, определенным в части первой настоящего пункта: получение наличных денежных средств в банкоматах и пунктах выдачи наличных денежных средств (кассах); операции, проведенные в пунктах выдачи наличных денежных средств (кассах), банкоматах, инфокиосках и СДБО Банка и других банков; переводы денежных средств с благотворительной карточки; зачисление денежных средств на благотворительную карточку; списание Банком вознаграждения со счета.

В случае отмены безналичной операции сумма, списанная в качестве пожертвования, возвращается на Счет в полном размере. В случае возврата денежных средств при отказе держателя карточки от оплаты товара, работы, услуги, в том числе по заявлению Клиента, сумма, списанная в качестве пожертвования, не возвращается на счет.

6. Клиент ознакомлен с тем, что доходы, полученные им в рамках рекламных игр и акций, а также иных рекламных мероприятий в виде подарка,

подлежат налогообложению подоходным налогом с физических лиц в соответствии с действующим законодательством.

ПОРЯДОК АКТИВАЦИИ И ИСПОЛЬЗОВАНИЯ БАНКОВСКОЙ ПЛАТЕЖНОЙ КАРТОЧКИ

7. Карточка является собственностью Банка (за исключением платежного кольца PayRing) и по окончании срока ее действия должна быть возвращена в Банк (за исключением виртуальной карточки и платежного кольца PayRing). Платежное кольцо PayRing является собственностью Клиента и передается Клиенту (его представителю), держателю дополнительной карточки после внесения вознаграждения с момента проставления им собственноручной подписи в заявлении-анкете под отметкой о выдаче платежного кольца PayRing.

Реквизиты виртуальной карточки отображаются Клиенту в системах дистанционного банковского обслуживания, определяемых Банком, код безопасности (CVV2/CVC2/КПП2-код) направляется SMS-сообщением на номер мобильного телефона Клиента, указанного в заявлении-анкете.

Вместе с карточкой (кроме виртуальной карточки) Клиенту (держателю дополнительной карточки) в запечатанном виде выдается конверт с ПИН-кодом, который генерируется автоматически в процессе персонализации карточки и используется для аутентификации клиента, держателя дополнительной карточки при проведении операций.

Выпуск карточки может осуществляться Банком без формирования конверта с ПИН-кодом с последующим предоставлением Клиенту (держателю карточки) ПИН-кода с использованием технологии e-PIN посредством направления SMS-сообщения на номер мобильного телефона Клиента (держателя дополнительной карточки). В данном случае для записи полученного значения ПИН-кода на микропроцессор карточки необходимо совершить любую успешную операцию с вводом ПИН-кода (получение наличных, просмотр баланса (доступного остатка) карточки) в банкомате Банка или иного банка, подключенного к ОАО «Банковский процессинговый центр».

Активация карточки (кроме виртуальной карточки) осуществляется в момент генерации ПИН-кода с использованием технологии e-PIN или – если указанная технология не применялась (ПИН-код выдан на бумажном носителе) – Клиентом (держателем дополнительной карточки) самостоятельно при совершении с использованием карточки следующих успешных операций, подтвержденных правильным вводом ПИН-кода: снятие наличных денежных средств; просмотр баланса (доступного остатка) по карточке; оплата товаров и услуг; смена ПИН-кода. Карточка не активируется в случае, если при проведении операции проверка ПИН-кода пройдена успешно, но сама операция отклонена (например, по причине недостаточности средств либо установления по карточке лимитов по проведению безналичных операций и (или) по получению наличных денежных средств); в случае неверного ввода

ПИН-кода; нахождения карточки в стоп-листе (блокировки карточки); при проведении с использованием карточки операции пополнения счета.

Активация бесконтактного интерфейса карточки осуществляется после успешно проведенной финансовой операции по карточке с использованием контактного микропроцессора с вводом правильного ПИН-кода (выдача наличных денежных средств, оплата и др.) в банкомате (инфокиоске), расположенном на территории Республики Беларусь, или терминале, установленном в Банке или организации торговли (сервиса) на территории Республики Беларусь.

При оформлении карточки Клиент указывает кодовое слово (девичью фамилию матери). При необходимости уточнения или изменения кодового слова Клиенту следует обратиться в отделение Банка с документом, удостоверяющим личность.

Клиент, держатель дополнительной карточки берет на себя обязательство держать в тайне реквизиты карточки и/или свой ПИН-код, а также хранить ПИН-код отдельно от карточки, так как введение ПИН-кода заменяет его подпись. Карточку имеет право использовать только Клиент, держатель дополнительной карточки, чьи имя, фамилия и/или подпись нанесены на карточку. Запрещается передавать карточку для использования третьим лицам.

При получении карточки с ПИН-кодом, направленным посредством SMS-сообщения при использовании технологии e-PIN, значение ПИН-кода приходит на зарегистрированный в Банке номер телефона.

8. Карточка либо ее реквизиты не должны использоваться в противозаконных целях, включая покупку товаров (работ, услуг), запрещенных законодательством Республики Беларусь, а также законодательством государства, на территории которого используется карточка.

Все операции с применением карточек или их реквизитов должны совершаться клиентами, держателями дополнительных карточек в пределах остатка денежных средств на счете и в рамках установленных лимитов совершения операций, а также с соблюдением иных ограничений, которые установлены или могут быть установлены Банком в соответствии с настоящими Правилами, Договором.

Подтверждением проведения операции, совершаемой с использованием карточки или ее реквизитов, являются карт-чек и (или) иные документы (в т.ч. выписки по счету), предусмотренные правилами платежной системы и (или) ЛПА. Карт-чеки и иные документы, являющиеся подтверждением проведения операций, совершаемых при использовании карточки или ее реквизитов, могут составляться на бумажном носителе и (или) в электронном виде.

При совершении операций с применением карточки или ее реквизитов средствами аутентификации Клиента, держателя дополнительной карточки являются ПИН-код, и (или) подпись Клиента, держателя дополнительной карточки на карт-чеке, и (или) иные средства аутентификации Клиента, держателя дополнительной карточки, предусмотренные правилами платежной системы, Банка и (или) Банка-эквайера. В случаях, предусмотренных

правилами платежной системы, возможно совершение операций по карточке без авторизации.

При проведении операции с использованием карточки Банк либо представитель ОТС вправе потребовать у Клиента, держателя дополнительной карточки предъявить документ, удостоверяющий личность.

При совершении операций при использовании карточек с бесконтактным интерфейсом возможно совершение операций без аутентификации.

Суммы всех операций, совершенных с применением карточки или ее реквизитов, отражаются по счету.

Совершение расходной операции с использованием карточки включает авторизацию по карточке и отражение операции по счету.

Момент совершения операции, как правило, не совпадает с моментом отражения операции по счету.

9. Совершение операций в банкоматах и других устройствах самообслуживания производится только с вводом ПИН-кода. Подписывая карт-чеки (вводя ПИН-код), держатель карточки признает правильность указанной в них суммы и тем самым дает указание Банку на осуществление операции по счету. При совершении операции допускается только три попытки неверного ввода ПИН-кода. При утрате ПИН-код не восстанавливается.

СРОК ДЕЙСТВИЯ КАРТОЧКИ

10. Карточка выдается на срок, указанный в заявлении-анкете на выпуск (перевыпуск) карточки. Срок действия карточки прекращается по истечении последнего числа месяца и года, указанных на карточке, после чего она должна быть возвращена в Банк. Не подлежат возврату в Банк виртуальная карточка и платежное кольцо PayRing.

При этом Банк вправе продолжить обслуживание карточки после истечения срока ее действия без проведения процедуры замены. О предпринятых действиях в отношении срока действия карточки Банк информирует Клиента путем направления SMS-сообщения.

В случае изъявления клиентом желания перевыпустить карточку в связи с окончанием срока действия специалист оформляет заявление-анкету и осуществляет необходимые действия для ее замены.

11. Если до истечения срока действия карточки на специальной полосе для хранения образца подписи (при ее наличии), расположенной на оборотной стороне карточки, проявилась надпись, свидетельствующая о недействительности карточки («VOID» для карточек международных платежных систем (далее – МПС) и «НЕДЕЙСТВИТЕЛЬНА» для карточек платежной системы БЕЛКАРТ), Клиенту, держателю дополнительной карточки необходимо обратиться в Банк для перевыпуска карточки. Клиент, держатель дополнительной карточки должен иметь ввиду, что представитель ОТС вправе отказать в приеме к оплате карточки, на которой имеется надпись, свидетельствующая о ее недействительности.

ИНФОРМАЦИОННО-КОНСУЛЬТАЦИОННАЯ ПОДДЕРЖКА

12. Контакт-центр Банка предоставляет следующую информацию по тел. 136:

стоимость выпуска и перевыпуска карточек Банка;

вознаграждение за операции, совершенные при использовании карточек Банка;

курсы валют, установленные для совершения валютно-обменных операций с использованием банковских платежных карточек Банка;

об услугах, предоставляемых держателям карточек Банка;

информационная поддержка в нестандартных ситуациях, возникающих при использовании карточки;

о местонахождении банкоматов, инфокиосков Банка.

13. Круглосуточная сервисная служба ОАО «Банковский процессинговый центр» (далее – служба сервиса (поддержки)) предоставляет следующие услуги:

внесение карточки в стоп-лист (блокировка) в случае ее утери, кражи, при подозрении на несанкционированное использование карточки или ее реквизитов по тел. +375 17 299 25 26;

изъятие карточки из стоп-листа, разблокировка карточки после превышения числа неверных попыток набора ПИН-кода, оказание консультаций информационно-справочного характера, управление жизненным циклом токена по тел. +375 17 299 25 25;

предоставление информации о доступной сумме по карточке по тел. +375 17 299 25 23.

СПОСОБЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ОБ ОСУЩЕСТВЛЕННЫХ С ИСПОЛЬЗОВАНИЕМ КАРТОЧКИ ОПЕРАЦИЯХ

14. Информацию об осуществленных с использованием карточки операциях Банк предоставляет Клиенту в виде выписки на бумажном носителе (выписка по счету) при личном обращении Клиента в Банк.

Дополнительно Банк предлагает следующие способы получения информации об осуществленных с использованием карточки операциях:

услуга «SMS-информирование» – позволяет получать посредством Push/SMS/Viber-сообщений информацию об операциях, совершенных при использовании карточки;

мини-выписка – формируемая Клиентом самостоятельно в устройствах самообслуживания, системах «Интернет-банкинг», «Мобильный интернет-банкинг» выписка, содержащая информацию о последних авторизационных запросах по карточке (не более 13 запросов), исключая просмотр баланса, за определенное количество дней (не более 9);

выписка по счету в СДБО – формируемая Клиентом самостоятельно в системах «Интернет-банкинг» и «Мобильный интернет-банкинг» выписка по счету;

ежемесячное направление Банком выписки по счету на адрес электронной почты Клиента, указанный в заявлении-анкете на выпуск карточки при открытии счета.

15. Способ получения информации об осуществленных с использованием карточки операциях указывается Клиентом в заявлении-анкете, которое является неотъемлемой частью Договора. В случае выявления неавторизованной операции Клиент обязан незамедлительно заблокировать карточку.

Датой получения Клиентом информации об осуществленных с использованием карточки операциях в случае опротестования Клиентом операции считается наиболее ранняя из следующих дат (определяется на основании сведений, зарегистрированных в информационных системах Банка или службе сервиса (поддержки), в зависимости от выбранного Клиентом способа информирования):

дата направления Банком Клиенту текстового сообщения на номер мобильного телефона в рамках подключенной Клиентом услуги «SMS-информирование»;

дата получения Клиентом мини-выписки в банкомате, инфокиоске, посредством систем «Интернет-банкинг», «Мобильный интернет-банкинг»;

дата получения Клиентом выписки, формируемой самостоятельно в системах «Интернет-банкинг» и «Мобильный интернет-банкинг»;

дата получения Клиентом выписки по счету на бумажном носителе при личном обращении в Банк (если Клиент не обращался за выпиской – первое число месяца, следующего за отчетным месяцем);

дата направления Банком выписки по счету на адрес электронной почты Клиента.

16. При выявлении несоответствия между отраженными в выписке и фактически осуществленными операциями держатель карточного платежного инструмента или Клиент имеет право требовать признания совершенной платежной операции неавторизованной в случаях, определенных законодательством и Национальным банком Республики Беларусь.

Заявление о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной должно быть предоставлено держателем карточного платежного инструмента или Клиентом в Банк на бумажном носителе в течение одного месяца с даты выявления факта неавторизованной операции, но не позднее 70 календарных дней с даты отражения этой операции по счету.

Банк вправе устанавливать перечень документов, подлежащих предоставлению держателем карточного платежного инструмента или Клиентом наряду с заявлением по неавторизованной операции в зависимости от характера оспариваемой операции, а также запрашивать дополнительные документы в процессе рассмотрения заявления держателя карточного платежного инструмента или Клиента. Непредставление держателем карточного платежного инструмента или Клиентом запрашиваемых Банком документов является основанием для отказа в проведении проверки.

Срок рассмотрения заявления о признании осуществленной с

использованием карточного платежного инструмента операции неавторизованной исчисляется со дня, следующего за днем регистрации заявления в Банке. Если последний день срока рассмотрения заявления приходится на нерабочий день, то днем истечения срока считается первый следующий за ним рабочий день.

Банк информирует держателя карточного платежного инструмента или Клиента о результатах рассмотрения заявления о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной в срок, не превышающий 90 календарных дней со дня регистрации заявления в Банке, путем направления держателю карточного платежного инструмента или Клиенту уведомления на бумажном носителе или в электронном виде. Уведомление о результатах рассмотрения заявления помимо прочего включает в себя:

сведения о принятом Банком решении о признании (непризнании) осуществленной с использованием карточного платежного инструмента операции неавторизованной;

основания, установленные законодательством в области платежных систем и платежных услуг, для отказа в признании осуществленной с использованием карточного платежного инструмента операции неавторизованной (в случае принятия соответствующего решения);

конкретную дату исполнения решения о возмещении суммы неавторизованной операции (в случае принятия соответствующего решения);

сумму денежных средств, причитающихся держателю карточного платежного инструмента или Клиенту в качестве возмещения.

17. Держатель карточного платежного инструмента или Клиент вправе требовать признания операции, осуществленной с использованием карточного платежного инструмента лицом, не являющимся держателем карточного платежного инструмента, неавторизованной, если осуществление этой операции стало возможным по причине компрометации карточного платежного инструмента в результате незаконного доступа к программно-техническим средствам банков, иностранных банков и (или) процессинговых центров и, как следствие, к реквизитам карточек и (или) информации, позволяющей несанкционированно использовать карточки.

Держатель карточного платежного инструмента или Клиент предоставляет в Банк заявление, содержащее требование о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной в соответствии с частью первой настоящего пункта, на бумажном носителе или в электронном виде. Подача такого заявления сроком не ограничивается.

При наличии у Банка информации о компрометации карточного платежного инструмента в случае, указанном в части первой настоящего пункта, заявление, содержащее требование о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной, подлежит обязательному удовлетворению Банком в части операций, осуществленных с использованием скомпрометированного карточного платежного инструмента, при условии соответствия заявленных

держателем карточного платежного инструмента или Клиентом реквизитов скомпрометированной карточки (аутентификационных данных) реквизитам (аутентификационным данным), имеющимся у Банка по каждому конкретному случаю компрометации карточного платежного инструмента, и отсутствия у Банка информации о причастности держателя карточного платежного инструмента или Клиента к организации незаконного доступа к программно-техническим средствам банков, иностранных банков и (или) процессинговых центров.

В случае если держателем карточного платежного инструмента или Клиентом по его инициативе была отменена блокировка скомпрометированного карточного платежного инструмента, осуществленная Банком в одностороннем порядке по причине компрометации карточного платежного инструмента в случае, указанном в части первой настоящего пункта, заявление, содержащее требование о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной, подлежит удовлетворению в части операций, осуществленных с использованием скомпрометированного карточного платежного инструмента до момента инициированной держателем карточного платежного инструмента или Клиентом отмены блокировки скомпрометированного карточного платежного инструмента.

В случае признания осуществленной с использованием карточного платежного инструмента операции, указанной в части первой настоящего пункта, неавторизованной Банк не взимает вознаграждение (плату) за подачу и рассмотрение заявления, включая проведение всех необходимых процедур в соответствии с правилами платежной системы, в рамках которых эмитирован карточный платежный инструмент.

Информирование держателя карточного платежного инструмента или Клиента о результатах рассмотрения заявления осуществляется согласно пункту 16 настоящих Правил.

Возмещение суммы неавторизованной операции осуществляется путем инициирования платежа в безналичной форме Банком в пользу Клиента.

Возмещение суммы неавторизованной операции осуществляется без взимания Банком вознаграждения (платы) за осуществляемые в целях обеспечения возмещения необходимые процедуры, расчетные операции.

18. Информация о доступной сумме по карточке Клиент, держатель дополнительной карточки может получить в службе сервиса (поддержки) по тел. +375 17 299 25 23, а также в СДБО.

УТЕРЯ КАРТОЧКИ ИЛИ ПИН-КОДА, СМЕНА ПИН-КОДА, БЛОКИРОВКА КАРТОЧКИ

19. Если карточка утрачена, украдена, постороннему лицу стали известны реквизиты карточки и (или) ПИН-код либо при выявлении осуществленных с использованием карточки неавторизованных операций или ее реквизитов Клиент, держатель дополнительной карточки должен незамедлительно заблокировать карточку в службе сервиса (поддержки) по

тел. +375 17 299 25 26(25), после чего уведомить Банк об этом в трехдневный срок для постановки карточки в жесткий стоп-лист путем предоставления заявления на бумажном носителе.

Карточка, которая передана или информация о которой передана в Банк третьими лицами, не являющимися клиентами, держателями дополнительных карточек (найденная карточка), подлежит обязательной блокировке работником Банка через службу сервиса (поддержки) по тел. +375 17 299 25 26.

20. Сменить ПИН-код карточки Клиент, держатель дополнительной карточки может, обратившись в любое Подразделение либо самостоятельно в СДБО. При этом ПИН-код будет направлен держателю карточки посредством SMS-сообщения при использовании технологии e-PIN.

Также Клиент, держатель дополнительной карточки может сменить ПИН-код карточки (за исключением карточек в формате форм-факторов) в банкоматах Банка.

За смену ПИН-кода Банк взимает вознаграждение, установленное Сборником платы (вознаграждений) за операции, осуществляемые Банком.

Также существует возможность запросить CVV2/CVC2/КПП2 виртуальной карточки в СДБО.

21. Новую карточку Банк выдает на основании заявления-анкеты на выпуск (перевыпуск) карточки, оформленного Клиентом на бумажном носителе либо с использованием СДБО, в соответствии с правилами Банка. За перевыпуск карточки Банк взимает вознаграждение, установленное Сборником платы (вознаграждений) за операции, осуществляемые Банком.

22. Клиент, держатель дополнительной карточки обязан предоставить по требованию Банка информацию для расследования обстоятельств утраты карточки. Если Банк имеет сведения о том, что незаконное использование карточки произошло с ведома Клиента, держателя дополнительной карточки, то ответственность за совершенные при использовании карточки операции несет Клиент, держатель дополнительной карточки.

При обнаружении карточки, ранее объявленной украденной или утерянной, использование такой карточки категорически запрещено.

23. Если карточка заблокирована по инициативе Банка или Клиента, держателя дополнительной карточки по причине ее компрометации, то Клиент, держатель дополнительной карточки вправе требовать от Банка разблокировать карточку в целях возобновления возможности ее использования. В случае поступления такого требования от Клиента, держателя дополнительной карточки Банк разблокирует карточку.

ОСОБЕННОСТИ СОВЕРШЕНИЯ ВАЛЮТНО-ОБМЕННЫХ ОПЕРАЦИЙ

24. Клиент до проведения валютно-обменных операций выражает свое согласие на использование при их проведении обменных курсов, установленных Банком, следующими способами:

при совершении операции с использованием СДБО – посредством подтверждения совершения операции с использованием обменных курсов

после ознакомления с ними;

при совершении операции в банкомате или инфокиоске Банка – посредством нажатия кнопки или выбора элемента интерфейса, которые инициируют совершение соответствующей операции;

при совершении иных операций:

если при совершении операции осуществляется аутентификация Клиента – посредством совершения действий для аутентификации Клиента;

если при совершении операции не осуществляется аутентификация Клиента – посредством совершения действий по инициированию совершения соответствующей операции либо действий по предоставлению третьим лицам права инициировать совершение соответствующей операции.

В случае если валюта операции не совпадает с валютой счета, а также в некоторых случаях, предусмотренных платежными системами, проводится валютно-обменная операция. Валютно-обменные операции совершаются по курсам, установленным Банком на момент совершения операции, с учетом кросс-курсов платежной системы «Мир» и МПС VISA и Mastercard. Для операций при использовании карточек Банка устанавливаются отдельные курсы валют, отличные от курсов по операциям с наличными денежными средствами. Валютно-обменные курсы для проведения операций при использовании карточек могут быть изменены в течение рабочего дня в соответствии с ЛПА Банка, регламентирующим установление курсов валют по операциям с использованием карточек. Информация об установленных Банком курсах валют по операциям с карточками размещается на главной странице корпоративного сайта Банка, в системах дистанционного банковского обслуживания клиентов (Интернет-банкинг, мобильный банкинг), а также в подразделениях Банка в общедоступном для Клиента месте.

Информация о курсах валют, установленных платежными системами, размещается на сайтах МПС VISA, Mastercard и платежной системы «Мир».

Для операций, совершенных за пределами Республики Беларусь или в устройствах банков, не подключенных к ОАО «Банковский процессинговый центр» (далее - БПЦ), момент совершения валютно-обменной операции определяется на основании расчетной информации, поступившей от платежной системы. В случае, когда платежная система в расчетной информации не указывает время совершения операции, для совершения такой операции применяют валютно-обменные курсы, установленные последним за эту дату распоряжением.

Для операций, совершенных в устройствах Банка или банков, подключенных к БПЦ, момент совершения валютно-обменной операции определяется исходя из даты и времени совершения операции.

По факту проведения Клиентом валютно-обменной операции Банк формирует документ, подтверждающий проведение валютно-обменной операции. Документ формируется (выводится на печать или интерфейс устройства) с использованием устройства Банка, в котором Клиентом проводится валютно-обменная операция. Данный документ содержит информацию, предусмотренную законодательством.

25. Обработка операций при использовании карточек производится в двух системах. Первоначально – в системе обработки авторизационных запросов, в которой в режиме реального времени изменяется доступная сумма по карточке (увеличивается либо уменьшается на сумму операции), а затем – в системе клиринга, в которой формируется расчетная информация. Только по мере обработки Банком расчетной информации сумма операции отражается по счету Клиента.

Поскольку обменные курсы устанавливаются МПС ежедневно и обновляются с учетом ситуации на валютном рынке, сумма операции в валюте счета на этапе авторизации и на этапе отражения операции по счету может отличаться (в меньшую или большую сторону).

26. При оплате в ОТС за пределами Республики Беларусь кассир может предложить клиенту выбрать валюту платежа, в которой будет совершаться операция. Среди предлагаемых валют указывается и валюта счета, к которому выпущена карточка. Необходимо учитывать, что в ходе таких операций помимо курсов банка-эмитента и МПС используются также курсы банка-эквайера, обслуживающего ОТС, что фактически увеличивает стоимость покупки. Например, если при совершении операции оплаты в Польше карточкой в долларах США в качестве валюты оплаты выбран доллар США, то сумма покупки в злотых будет переведена в доллары США по курсу банка-эквайера, обслуживающего ОТС, который, как правило, менее выгоден, чем курс МПС. Во избежание излишних расходов рекомендуем при оплате в ОТС выбирать валюту той страны, в которой производится оплата.

27. При возврате на счет денежных средств по валютно-обменной операции при использовании карточки порядок применения валютно-обменных курсов зависит от типа операции и даты операции, которые указываются банком-эквайером, обслуживающим ОТС.

28. При зачислении на счет денежных средств, поступивших по банковскому переводу в валюте, отличной от валюты счета, Банком осуществляются валютно-обменные операции по курсам, установленным для проведения операций с использованием карточек на момент совершения операций.

ОСОБЕННОСТИ СОВЕРШЕНИЯ ОПЕРАЦИЙ В ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ

29. Термины:

3D-Secure – дополнительная технология аутентификации при совершении операции оплаты товаров, работ и услуг в глобальной компьютерной сети Интернет при использовании карточек, на базе которой МПС разработаны специальные программы – Verified by VISA и Mastercard SecureCode; платежной системой БЕЛКАРТ разработана аналогичная технология – БЕЛКАРТ-ИнтернетПароль, также платежной системой «Мир» разработана технология MirAccept.

CVV2/CVC2/КПП2 – трехзначный код проверки подлинности карточки, который наносится на полосу для подписи и используется в качестве

защитного элемента при проведении операций в глобальной компьютерной сети Интернет.

30. Банк предоставляет Клиенту, держателю дополнительной карточки, эмитированной Банком, возможность совершения операций оплаты товаров, работ и услуг в глобальной компьютерной сети Интернет с применением реквизитов карточки с учетом следующих особенностей:

Банк предоставляет Клиенту, держателю дополнительной карточки возможность использования технологий 3D-Secure и БЕЛКАРТ-ИнтернетПароль;

для подтверждения совершения операции в глобальной компьютерной сети Интернет как правило используется CVV2/CVC2/КПП2, однако при совершении повторных (подписанных) платежей в одной и той же ОТС допускается отсутствие подтверждения CVV2/CVC2/КПП2.

В соответствии с разработанной МПС Mastercard технологией выгрузки данных по программе автоматического обновления данных (Automatic Billing Updater – ABU), обязательной для всех банков-участников, Банк обязан передать реквизиты выпущенных (перевыпущенных) карточек (за исключением CVC2/CVV2/КПП2 кода) в систему, обеспечивающую обновление реквизитов карточек в интернет-магазинах и сервисах. Клиент, держатель дополнительной карточки может отказаться от передачи реквизитов выпущенной (перевыпущенной) карточки путем предоставления письменного заявления произвольной формы, обратившись в любое Подразделение.

Банк имеет право устанавливать ограничения на совершение операций оплаты товаров, работ и услуг в глобальной компьютерной сети Интернет (в том числе с применением технологий 3D-Secure и БЕЛКАРТ-ИнтернетПароль) при использовании карточек.

31. Клиент, держатель дополнительной карточки несет ответственность за операции, совершенные с использованием своей карточки или ее реквизитов в глобальной компьютерной сети Интернет (далее – Интернет-платежи), а также за все суммы, списанные со счета в результате совершения Интернет-платежей.

Клиент, держатель дополнительной карточки несет все риски, связанные с проведением Интернет-платежей и осуществлением иных действий, связанных с внесением и сохранением реквизитов карточки на Интернет-сайтах.

Клиент, держатель дополнительной карточки не может предъявлять Банку претензии по операциям, проведенным в глобальной компьютерной сети Интернет при использовании карточки, в случае нарушения настоящих Правил.

Банк не несет ответственность в случае невозможности проведения Клиентом, держателем дополнительной карточки Интернет-платежей по независящим от Банка обстоятельствам.

Введение правильных реквизитов карточки, кода CVV2/CVC2/КПП2 и/или проверочного кода 3D-Secure является надлежащей и достаточной аутентификацией держателя карточки для отражения по Счету операции,

совершенной при использовании карточки и ее реквизитов.

31-1. Раскрытие информации в соответствии со статьей 23 Закона Республики Беларусь от 19.04.2022 № 164-З «О платежных системах и платежных услугах» производится Банком посредством размещения Правил платежной системы ОАО «Белагропромбанк» на официальном сайте Банка в глобальной компьютерной сети Интернет по адресу: www.belapb.by.

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ КАРТОЧКИ

32. Общие рекомендации.

32.1. При получении карточки распишитесь на ее оборотной стороне в специальном поле, при его наличии. Наличие подписи на карточке снизит риск использования ее другими лицами в случае ее утери, кражи. При отсутствии подписи на карточке либо несоответствии подписи образцу на карточке и документах, удостоверяющих личность, в проведении операции может быть отказано, а карточка изъята.

32.2. Сохраните номер телефона службы сервиса (поддержки) карточек Банка в легкодоступном месте (например, в памяти мобильного телефона или записной книжке), эта информация может пригодиться для блокировки карточки в случае ее утери либо кражи.

32.3. Для осуществления каждого типа операций (ежедневных и/или регулярных операций, платежей в глобальной компьютерной сети Интернет, операций в зарубежных поездках) выпустите отдельные карточки к различным счетам. Для осуществления платежей за рубежом желательно оформить к одному счету несколько карточек различных платежных систем и хранить карточки отдельно друг от друга.

Помните, что не стоит хранить большие суммы денег на карточках, которыми вы пользуетесь нерегулярно: например, карточку для оплаты в глобальной компьютерной сети Интернет стоит пополнять именно на ту сумму, которую планируете потратить, и непосредственно перед совершением платежа.

32.4. Обеспечивайте условия хранения карточки, которые исключают возможность ее утери, порчи, копирования данных, несанкционированного и незаконного использования. Не допускайте механических повреждений на карточке, деформации, загрязнения, воздействия высоких и низких температур, электромагнитных полей, прямых солнечных лучей, влаги, красителей, растворителей, вредных химических веществ и других неблагоприятных факторов, которые могут повлечь неработоспособность карточки.

32.5. Не передавайте карточку третьим лицам. Право пользования карточкой имеет только лицо, чьи персональные данные указаны на лицевой стороне карточки, если Договором и правилами платежной системы не установлено, что фамилия, имя держателя карточки могут не указываться. При необходимости предоставления доступа к своему счету иным лицам можно обратиться в Банк для оформления дополнительных карточек к счету.

32.6. Храните в тайне от других лиц конфиденциальные данные

карточки: номер и срок действия карточки, указанный на оборотной стороне трехзначный код проверки подлинности карточки (при его наличии), ПИН-код, который необходимо запомнить или, в случае если это является затруднительным, хранить его отдельно от карточки в неявном виде (например, переписав его на листок бумаги среди прочих групп цифр или любой другой информации). Никогда не сообщайте ПИН-код другим лицам, включая родственников, знакомых, работников банков, ОТС, представителей правоохранительных органов. Не передавайте ПИН-код ни по телефону, ни по электронной почте. Только Клиент, держатель дополнительной карточки должен знать свой ПИН-код.

32.7. Настоятельно рекомендуем использовать услугу «SMS-информирование», которая обеспечивает оперативное получение информации о совершенных по карточке операциях. Услуга «SMS-информирование» позволяет посредством текстового сообщения на мобильный телефон оперативно информировать о состоянии счета, изменении остатка по счету. При поступлении Push/SMS/Viber-сообщения об операции, которую Вы не совершали, необходимо незамедлительно заблокировать карточку и обратиться в Банк.

Если при наличии подключенной услуги «SMS-информирование» сообщения от Банка о проводимых операциях перестали поступать на Ваш мобильный телефон, необходимо связаться с Банком для уточнения причин, чтобы исключить возможность перехвата Push/SMS/Viber-сообщений третьими лицами. Если полученное Push/SMS/Viber-сообщение вызывает какие-либо сомнения или опасения, оперативно обратитесь в Банк для получения разъяснений.

32.8. Для взаимодействия с Банком используйте только реквизиты средств связи (мобильных и стационарных телефонов, факсов, Интернет-сайтов, обычной и электронной почты), которые указаны в документах, полученных непосредственно в Банке.

32.9. При утере, краже карточки, оставлении ее в банкомате или ином устройстве самообслуживания, изъятии кассиром ОТС, компрометации карточки (если конфиденциальные данные карточки стали известны посторонним лицам) либо при возникновении таких подозрений необходимо немедленно заблокировать карточку (например, позвонив в службу сервиса (поддержки), или посредством СДБО) и обратитесь в Банк.

32.10. Сохраняйте карт-чеки и иные документы по операциям с карточкой для сверки с выпиской по счету. Старайтесь проверять состояние счета регулярно, не реже чем раз в месяц, а также после заграничных поездок, в которых использовалась карточка. При выявлении расхождений между фактически совершенными и отраженными в выписке операциями обратитесь в Банк для уточнения обоснованности операций.

32.11. Используйте предлагаемые Банком возможности по установлению лимитов по операциям. Рекомендуется отключить или лимитировать возможность оплаты карточкой в глобальной компьютерной сети Интернет, а также совершения операций за рубежом, если вы не планируете совершать данные операции в ближайшее время.

33. Проведение операций при использовании карточки в банкоматах и инфокиосках.

33.1. При выборе банкомата или инфокиоска, в котором вы собираетесь провести операцию при использовании карточки, желательно избегать плохо освещенных и безлюдных мест. Наиболее безопасными местами для совершения операций являются помещения банковских офисов, уличные же банкоматы в туристических районах являются менее безопасными.

33.2. Для совершения регулярных операций старайтесь пользоваться одним и тем же банкоматом, расположенным в хорошо освещенном месте: вам будет проще выявить факт установки на него стороннего оборудования, которое может использоваться мошенниками для похищения информации с карточек.

33.3. Перед началом обслуживания осмотрите лицевую панель банкомата. Банкоматы некоторых банков предлагают сверить изображение банкомата на мониторе с тем, который перед вами. Обратите особое внимание на щель картоприемника: мошенники могут установить на него не предусмотренную конструкцией банкомата накладку. Перед использованием банкомата или другого устройства самообслуживания потрогайте панели, попробуйте их подвигать: фальшивые накладки и клавиатуры обычно держатся плохо и, как правило, даже при незначительном воздействии шатаются, отходят или даже отпадают. Зачастую мошенники оставляют заметные следы: щели, клеевые подтеки и сколы. Лучше не использовать банкомат, картоприемник которого выглядит так, будто кто-то ковырял его отверткой или облил клеем.

Порой мошенники делают поддельные панели с видеокамерами, которые затем крепятся к банкомату: на диспенсер для денег, под козырек, под экран или даже в стенде для рекламных брошюр. Эти камеры издалека могут выглядеть как черные точки.

Если клавиатура неестественно выпирает, шатается или отличается по тону, выглядит новой, в то время как сам банкомат уже имеет явные признаки изношенности, – это также повод отказаться от использования такого устройства самообслуживания.

33.4. Не применяйте чрезмерную физическую силу, чтобы вставить карточку в банкомат (инфокиоск). Если банковская карточка не вставляется без дополнительных усилий, воздержитесь от использования данного банкомата (инфокиоска).

В некоторых банкоматах (инфокиосках) могут применяться специальные устройства, которые препятствуют копированию мошенниками данных о карточках, – джиттеры. В таких банкоматах (инфокиосках) процесс приема карточек устройством может отличаться от других банкоматов (инфокиосков) – карточка вибрирует в момент ее приема устройством.

33.5. При обнаружении постороннего оборудования (например, накладки) не пытайтесь снять его самостоятельно, воздержитесь от совершения операций, а о выявленной накладке сообщите в банк, обслуживающий устройство. Если сомнения относительно корректной работы банкомата или другого устройства самообслуживания возникли после того,

как карточка помещена в картоприемник, не вводите ПИН-код. Нажмите кнопку для отмены операции и заберите карточку. Если вы заметили постороннее оборудование уже после окончания обслуживания, обязательно сразу же заблокируйте карточку любым доступным способом.

33.6. Убедитесь, что выбранный вами банкомат или другое устройство самообслуживания принимает имеющуюся у вас карточку. Логотип на вашей карточке и на экране программно-технического устройства и (или) на его корпусе должны быть одинаковы. Если вы вставили в банкомат или другое устройство самообслуживания карточку, не обсуживающуюся в данном устройстве, карточка будет вам возвращена, при этом на экране появится информация о невозможности совершения операции.

33.7. В случае если поблизости от банкомата или другого устройства самообслуживания находятся люди, вызывающие у вас подозрение, следует выбрать другое время для использования данного устройства или воспользоваться другим банкоматом или устройством самообслуживания.

33.8. Будьте особенно осторожны, если незнакомые люди предлагают вам помощь в использовании карточки в банкомате или другом устройстве самообслуживания. В случае затруднений, возникших при использовании карточки, не прислушивайтесь к советам посторонних лиц, а для связи с Банком пользуйтесь только номерами телефонов, которые указаны непосредственно на карточке либо получены вами из надежных проверенных источников или непосредственно в Банке.

33.9. Обращайте внимание на людей, стоящих за вами в очереди у банкомата или другого устройства самообслуживания, в случае необходимости попросите их отойти на расстояние, с которого они не смогут увидеть вводимый вами ПИН-код. При вводе ПИН-кода находитесь как можно ближе к банкомату или устройству самообслуживания, при этом прикрывайте клавиатуру ладонью свободной руки.

33.10. При использовании карточки внимательно изучайте информацию, выводимую на экран банкомата или другого устройства самообслуживания, и проверяйте правильность вводимых данных. При неоднократном некорректном вводе ПИН-кода карточка блокируется и может быть изъята банкоматом или другим устройством самообслуживания. В случае изъятия карточки (независимо от причины) банкоматом или другим устройством самообслуживания немедленно заблокируйте ее (например, связавшись со службой сервиса (поддержки) или с использованием СДБО).

33.11. Не позволяйте никому отвлекать вас во время проведения операции, поскольку вы можете случайно совершить некорректную операцию. Кроме того, при отсутствии каких-либо действий с вашей стороны в течение установленного для данного устройства времени оно может изъять вашу карточку и (или) деньги.

33.12. После получения наличных денежных средств в банкомате следует убедиться в том, что карточка была возвращена банкоматом, дождаться выдачи карт-чека (при его запросе) и только после этого отходить от банкомата. Следует помнить, что последовательность выдачи наличных денежных средств и возврата карточки в банкоматах разных банков может

отличаться. Банкомат может сначала вернуть карточку, а затем выдать запрошенную сумму денежных средств. Необходимо учитывать данную специфику работы банкоматов и не отходить от устройства до момента получения карточки, карт-чека (при его запросе) и денег.

33.13. В случае если банкомат или другое устройство самообслуживания работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого устройства, отменить совершаемую операцию, нажав на клавиатуре соответствующую кнопку, и дождаться возврата карточки. Если устройство не возвращает карточку, следует незамедлительно заблокировать карточку любым доступным способом и обратиться в Банк.

33.14. Не оставляйте запрошенный вами карт-чек в банкомате или другом устройстве самообслуживания, так как в чеке могут быть указаны сумма операции, остаток денежных средств. Это может привлечь грабителя или мошенника.

34. Получение наличных денежных средств и проведение операций безналичной оплаты при использовании карточки в отделениях банков.

34.1. Все действия работника банка с карточкой должны проходить под вашим наблюдением. Не разрешайте работнику банка уходить с карточкой в другое помещение.

34.2. При получении наличных денежных средств либо проведении безналичной оплаты особое внимание обращайте на соответствие указанной суммы и суммы, содержащейся в карт-чеке (слипе).

34.3. Работник банка вправе потребовать предъявления документа, удостоверяющего личность, для идентификации держателя карточки и оформления операции.

34.4. При проведении операций в ПВН обращайте особое внимание на действия работника банка, если он пытается провести вашу карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение неавторизованных операций. Обязательно поинтересуйтесь причиной, по которой работнику необходимо повторно провести карточку через считывающее устройство оборудования.

33.5. Перед вводом ПИН-кода внимательно изучите информацию, представленную на экране терминала, а также убедитесь, что сумма и валюта операции верны.

34.6. Вводите ПИН-код, прикрывая клавиатуру ладонью свободной руки. Никогда и ни при каких обстоятельствах не сообщайте ПИН-код работникам банка.

34.7. Перед тем как подписать карт-чек, убедитесь, что сумма и валюта операции, дата операции, тип операции и другие данные, указанные в карт-чеке, верны.

35. Проведение операций безналичной оплаты при использовании карточки в ОТС.

35.1. Используйте карточки в ОТС, которые вызывают доверие.

35.2. При проведении операций в ресторанах, барах, магазинах, отдавая карточку обслуживающему персоналу, не выпускайте ее из поля зрения. При

необходимости проследуйте за работником ОТС к терминалу. Это позволит предотвратить неправомерное копирование информации, указанной на карточке.

35.3. При совершении операции с использованием принтера или платежного терминала (POS-терминала) кассир может потребовать ввести ПИН-код или подписать карт-чек в соответствии с требованиями, установленными правилами платежных систем, в рамках которых эмитируются карточки, а также предоставить документ, удостоверяющий личность, в целях идентификации личности держателя карточки.

35.4. При проведении операции оплаты в ОТС обращайте особое внимание на действия кассира, если он пытается провести карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение несанкционированных операций. Обязательно поинтересуйтесь причиной, по которой кассиру необходимо повторно провести карточку через считывающее устройство оборудования. Если вследствие неуспешной операции по карточке вы оплатили покупку иным способом (например, наличными или иной карточкой), сохраните подтверждающий документ и проверьте, списались ли со счета денежные средства по неуспешной операции.

35.5. Вводите ПИН-код, прикрывая клавиатуру ладонью свободной руки. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости от Вас, не смогут его увидеть. Никогда и ни при каких обстоятельствах не сообщайте ПИН-код работникам ОТС.

35.6. Перед тем как подписать карт-чек, убедитесь, что сумма и валюта операции, номер карточки (его часть), дата операции, тип операции, название ОТС и другие данные, указанные в карт-чеке, верны.

35.7. Если вы решили отказаться от покупки после успешного завершения операции, потребуйте отменить операцию. Обязательно сохраните карт-чек по операции отмены до сверки выписки по счету, к которому выпущена карточка.

35.8. Бесконтактные операции совершаются в режиме «самообслуживания»: Клиент, держатель дополнительной карточки не передает карточку или другой платежный инструмент, используемый для оплаты (например, браслет, брелок, мобильный телефонов или другое устройство) кассиру, а самостоятельно прикладывает карточку или другой платежный инструмент к считывающему устройству терминала для проведения операции.

36. Проведение операций безналичной оплаты при использовании карточки в глобальной компьютерной сети Интернет.

36.1. Не используйте для оплаты в Интернете карточки, на которых у Вас находятся крупные суммы денег. Для таких целей лучше завести отдельную карточку (к отдельному счету) и переводить туда деньги только по мере необходимости. При использовании виртуальной карточки рекомендуем не использовать ее для хранения денежных средств, а пополнять карточку по мере необходимости.

36.2. Для обеспечения наиболее высокого уровня безопасности операций подключите услугу подтверждения операций по технологии 3D-Secure и/или БЕЛКАРТ-ИнтернетПароль. Данные технологии позволяют запросить дополнительное подтверждение операций, совершаемых в глобальной компьютерной сети Интернет, с помощью одноразового пароля, высылаемого на телефон (посредством Push/SMS/Viber-сообщения), указанный при подключении услуги.

Сайт интернет-магазина, обеспечивающий прием платежей с применением технологий 3D-Secure и БЕЛКАРТ-ИнтернетПароль, как правило, должен размещать логотипы соответствующих программ платежных систем.

36.3. Не отвечайте на электронные письма, в которых от имени якобы Банка или иных организаций, а также граждан просят предоставить персональную информацию, в том числе реквизиты карточки, в целях их обновления или для регистрации. Постарайтесь выяснить правомерность таких предложений, связавшись с Банком по достоверно известному номеру телефона (например, полученному вами непосредственно от Банка при получении карточки).

Передавайте информацию о своей карточке только для оплаты покупки. Никогда не пересылайте данные карточки по электронной почте, так как передаваемая по электронной почте информация не полностью защищена от перехвата и использования посторонними. На сайтах всех известных благонадежных магазинов используется технология шифрования данных, которая защищает Вашу информацию личного характера при совершении покупки.

Никогда не показывайте номер карточки в доказательство достижения Вами определенного возраста, хотя иногда на некоторых сайтах могут попросить это сделать. Номер карточки не может указывать на достижение Вами какого-либо возраста.

36.4. Злоумышленники часто распространяют вирусные программы через различные Интернет-ресурсы – от социальных сетей до обычных новостных сайтов. Клиент, компьютер которого заражен, при попытке войти в личный кабинет может быть незаметно перенаправлен на «фишинговый» сайт, который внешне практически не отличается от подлинных сайтов Интернет-банков, интернет-магазинов или других платежных сервисов. Чтобы этого избежать, старайтесь максимально использовать возможности вашего браузера и почтового клиента по обеспечению безопасности. Для этого в опциях браузера и почтового клиента необходимо включить дополнительные функции. Например, «Блокировка всплывающих окон», «Защита от фишинга и вредоносного ПО», «Открывать файлы на основе содержимого, а не расширения» и др. Также не стоит пользоваться окном предварительного просмотра в используемом вами почтовом клиенте.

Кроме того, рекомендуется всегда самостоятельно вводить веб-адрес банка («Интернет-банкинга») в адресную строку браузера вместо использования любых гиперссылок, тем более из подозрительных сообщений.

36.5. Делайте покупки в известных Вам интернет-магазинах или сначала

убедитесь в том, что они пользуются хорошей репутацией и надежны. Проверяйте правильность адресов Интернет-сайтов, к которым подключаетесь для совершения покупки, так как похожие адреса могут использоваться для осуществления неправомерных действий. Если у вас появились какие-либо подозрения относительно Интернет-страницы или вы не хотите предоставлять персональные или карточные данные, то покиньте страницу и произведите покупку в другом месте.

Во время совершения оплаты по карточке в глобальной компьютерной сети Интернет удостоверьтесь, что фрагмент веб-адреса «http» в адресной строке веб-браузера изменился на «https» — это будет означать, что сессия зашифрована. Большинство браузеров дополнительно визуализируют такое изменение изображением навесного замка, кликнув по которому, можно просмотреть сертификаты, подтверждающие безопасность расчетов через данный сайт.

36.6. Перед совершением операции оплаты товара (услуги) внимательно изучите условия предлагаемого соглашения, в частности, все правила предоставления услуг, условия доставки, возврата, замены товара, а также процедуру отмены заказа. Особенно внимательно читайте условия совершения операций, связанных с азартными играми (казино, лотереи), так как они могут предусматривать автоматическую подписку, что повлечет списание денежных средств на регулярной основе. Отдельно оцените целесообразность совершения операции, если информация об условиях покупки изложена на незнакомом языке. Найдите номер телефона или адрес электронной почты ОТС и запишите их на случай, если у Вас возникнут вопросы.

36.7. Ведите учет операций, совершенных в глобальной компьютерной сети Интернет, включая адреса сайтов интернет-магазинов. Многие интернет-магазины посылают покупателям электронные сообщения с обобщающей информацией об операциях – сохраните или распечатайте их. Сохраняйте любые электронные документы, переписку по электронной почте, касающуюся попыток разрешения спорной ситуации с ОТС, так как данные документы могут оказаться очень важны для защиты ваших прав. При невозможности самостоятельно разрешить спорную ситуацию обратитесь в Банк.

36.8. Некоторые ОТС (например, гостиницы, пункты проката автомобилей) имеют право запрашивать авторизацию по карточке до продажи товара, выполнения работ и оказания услуг в качестве гарантии платежеспособности держателя карточки. В результате авторизации запрошенная сумма блокируется на карточке Клиента, держателя дополнительной карточки и становится недоступной.

36.9. Если было произведено бронирование гостиницы через Интернет-сайт, но по каким-то причинам не планируется воспользоваться ею, обязательно проведите отмену бронирования через тот же Интернет-сайт согласно указанным на нем процедурам. Получение Клиентом, держателем дополнительной карточки кода отмены бронирования отеля является доказательством того, что бронь действительно отменена. В ином случае за

несвоевременную отмену брони гостиница имеет право представить к списанию со счета сумму денежных средств в установленном ею размере.

36.10. Никогда не сообщайте свой ПИН-код при заказе товаров по телефону или почте и не вводите его нигде в Интернете. Для совершения подобных операций ПИН-код никогда не используется.

36.11. Убедитесь в том, что проводимые Вами операции соответствуют закону. Если на сайте интернет-казино или на других сайтах азартных игр присутствуют логотипы платежных систем, то это НЕ означает, что проведение операций, связанных с участием в азартных играх, правомерно. Если у Вас возникли какие-либо вопросы или сомнения в правомерности совершаемых операций, обратитесь в Банк.

36.12. Совершайте покупки только со своих устройств, не пользуйтесь Интернет-кафе и другими общедоступными средствами, где могут быть установлены программы-шпионы, запоминающие вводимые Вами конфиденциальные данные.

36.13. Устанавливайте на свои устройства лицензионное программное обеспечение, в том числе антивирусное, и межсетевые экраны (фаерволы/брандмауэры) и регулярно производите их обновление. Это поможет защитить ваши устройства от вирусов и других деструктивных программ, а также от несанкционированного доступа к вашим конфиденциальным данным. Даже если вы уверены в своем программном обеспечении, не стоит открывать или загружать вложения электронных писем от незнакомых и сомнительных адресатов.

36.14. Подключитесь к услугам Банка, позволяющим осуществлять оперативный контроль за расходами по своей карточке («Интернет-банкинг», «Мобильный интернет-банкинг», «SMS-информирование» и пр.).

36.15. При появлении подозрений о неправомерном списании денег рекомендуем незамедлительно осуществить блокировку Вашей карточки и обратиться в Банк.

37. Использование СДБО.

37.1. Храните в тайне от других лиц конфиденциальные данные карточки: номер и срок действия карточки, указанный на оборотной стороне трехзначный код проверки подлинности карточки (при его наличии), а также сведения, касающиеся учетных записей в СДБО: логины, пароли, коды доступа, данные из Push/SMS/Viber-сообщений и т.д.

37.2. При использовании системы «Интернет-банкинг» обращайте внимание на наличие на странице сервиса защищенного протокола HTTPS. Перед входом в систему рекомендуется удостовериться в подлинности сертификата и сайта. Как правило, для этого необходимо кликнуть в поле адресной строки Интернет (поле с пиктограммой замка или листа бумаги) и сверить имеющуюся в блоке информацию. В случае несоответствия присутствующих данных с реальными сведениями о Банке стоит немедленно покинуть страницу.

37.3. Не забывайте периодически (а также в случае, если пароль стал известен посторонним лицам) менять свой пароль. Старайтесь сделать его максимально сложным и уникальным. Для этого используйте в пароле

прописные и строчные буквы, цифры и символы. Не используйте один и тот же пароль в разных системах (электронная почта, системы «Интернет-банкинг» других банков, социальные сети и т.п.). Постарайтесь избегать в пароле даты своего рождения, имени и других доступных о вас данных. Ни при каких обстоятельствах не разглашайте свой пароль никому, включая сотрудников банка.

37.4. Будьте осторожны, посещая сайты с сомнительным содержанием: именно они, как правило, являются источником самых новых вирусов.

37.5. По окончании сеанса работы с системой «Интернет-банкинг» обязательно корректно выходите из системы, используя соответствующую опцию.

38. Проведение операций с использованием приложений и «Мобильный интернет-банкинг».

38.1. Устанавливайте мобильные приложения (в том числе и приложения Банка) только из известных источников (Google Play, Windows Store, App Store или AppGallery). Рекомендуется использовать антивирус для мобильных устройств.

38.2. Помните, что Банк не рассылает своим Клиентам, держателям дополнительных карточек ссылки или указания на установку приложений через Push/SMS/Viber/MMS/e-mail-сообщения.

38.3. Не устанавливайте мобильные приложения Банка на мобильный телефон (устройство), на котором получены root-права (права суперпользователя). Такие телефоны и устройства также не рекомендуется использовать для получения сообщений от Банка (например, SMS с кодом (одноразовым паролем) для прохождения аутентификации).

38.4. При утрате мобильного телефона (устройства), на котором установлено мобильное приложение Банка (приходят Push/SMS/Viber-сообщения с подтверждающими одноразовыми паролями), или неожиданном прекращении работы SIM-карты следует как можно быстрей заблокировать SIM-карту.

39. Особенности проведения операций при использовании карточки.

39.1. Необходимо учитывать, что специфика совершения операций при использовании карточки предполагает наличие временного разрыва между датой совершения операции и отражения данной операции по счету. Продолжительность периода между днем совершения операции и днем отражения операции по счету зависит от места осуществления операции (на территории Республики Беларусь или за границей), принадлежности технической инфраструктуры (Банку или другому банку), времени осуществления операции (ночное или дневное время, рабочие или выходные, праздничные дни).

39.2. В зависимости от страны пребывания и банка при проведении операции при использовании карточки может удерживаться дополнительное вознаграждение, о размерах которого целесообразно поинтересоваться у обслуживающего вас работника перед совершением операции либо заранее изучив информацию банка на его официальном сайте. Также такая информация может быть отображена на экране банкомата или устройства

самообслуживания при совершении операции.

39.3. В случае если вы все же пострадали от мошенничества, необходимо немедленно заблокировать карточку и обратиться в Банк. По факту мошенничества необходимо подать заявление в правоохранительные органы.

39.4. При совершении операций оплаты товаров, работ и услуг, снятия наличных за границей стоит обращать внимание на наличие сервиса Dynamic currency conversion (DCC), что в переводе означает «динамический обмен валюты». Этот сервис предлагает дополнительный этап конверсии, что, как правило, приводит к уплате дополнительной комиссии: сумма к оплате пересчитывается в валюту страны, в которой эмитирована карточка, по курсу, установленному банком, предлагающим услугу DCC. Необходимо внимательно следить за информацией, представленной на экране терминала, а также проверять указанные в карт-чеке условия проведения операции (в частности, стоит обращать внимание на наличие аббревиатуры DCC). В случае несогласия с условиями проведения операции настаивайте на отмене операции и ее проведении без применения динамической конверсии. В случае несогласия работников организации отменить операцию с использованием динамической конверсии стоит, не покидая организации, обратиться в полицию.

ГАРАНТИЙНОЕ ОБСЛУЖИВАНИЕ ПЛАТЕЖНОГО КОЛЬЦА PAYRING

40. При оформлении платежного кольца PayRing в отношении кольца осуществляется гарантийное обслуживание сроком на 12 месяцев. Исчисление гарантийного срока начинается с момента передачи платежного кольца PayRing Клиенту, держателю дополнительной карточки, о чем в заявлении-анкете под отметкой о получении карточки Клиентом, держателем дополнительной карточки проставляется собственноручная подпись.

К гарантийным случаям относится неработоспособность платежного кольца PayRing при совершении операций в связи с заводским браком.

По истечении срока гарантийного обслуживания перевыпуск платежного кольца PayRing осуществляется согласно со Сборником платы (вознаграждений) за операции, осуществляемые Банком.

Гарантийное обслуживание платежного кольца PayRing не распространяется на:

естественный износ и старение (царапины, сколы);

повреждения в результате небрежного использования (удары, вмятины);

повреждения при взаимодействиях с агрессивными жидкостями, в том числе косметическими (растворители, антисептики, средства с содержанием свинца и т.п.);

повреждения при взаимодействии с мощными электромагнитными и магнитными полями;

повреждения, вызванные при погружении в воду на глубину свыше 3 метров.