«УТВЕРЖДЕНО»
решением Правления
(протокол № 32 от «15» октября 2026 г.)
и приказом № 1-15/10 от «15» октября 2026 г.
АО «Национальный межбанковский
процессинговый центр»

ПРАВИЛА
НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ
«HUMO»

(версия 1.0.3 от 15.10.2026)

Ташкент 2026

Содержание:

1. Общие положения 3
1.1. Введение 3
1.2. Термины и определения 3
1.3. Обязательность Правил и их применение 7
1.4. Взаимодействие Оператора с иными платежными системами 8
2. Товарные знаки, знаки обслуживания, логотипы и правила их использования 8
3. Взаимодействие между Оператором, Участниками и Платежными организациями 10
3.1. Права и обязанности Оператора 10
3.2. Права и обязанности Участников 12
3.3. Права и обязанности Платежной организации 14
4. Порядок ведения перечня Участников 16
5. Процедуры вступления и выхода из Системы 16
5.1. Порядок вступления Участника в Систему 16
5.2. Порядок приостановления и прекращения участия в Системе 17
6. Эмиссионная деятельность 19
6.1. Права и обязанности Эмитента 19
6.2. Порядок предоставления БИНов 20
6.3. Требования к договору Эмитента с Клиентом 21
7. Эквайринговая деятельность 22
7.1. Права и обязанности Эквайера 22
7.2. Взаимодействие Эквайера с ТСП 24
7.3. Требования к оформлению и функционалу Интернет–сайта ТСП для приёма оплаты с использованием реквизитов Карт (интернет-эквайринг) 25
7.4. Требования к оформлению мест обслуживания Карт 26
7.5. Правила проверки ТСП 26
7.6. Правила присвоения MCC-кодов 26
7.7. Порядок работы с изъятыми Картами 27
8. Мероприятия по противодействию мошенничеству, Операциям, связанным с незаконной игорной деятельностью и иным Операциям повышенного риска 27
8.1. Антифрод мероприятия 27
8.2. Мероприятия по противодействию Операциям, связанным с незаконной игорной деятельностью и иным Операциям повышенного риска 31
9. Система управления рисками в Системе 32
10. Требования к обеспечению защиты информации 33
10.1. Требования к Участникам Системы по защите информации 34
10.2. Выявление Инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении Операций в Системе 36
10.3. Обеспечение совершенствования защиты информации при осуществлении Операций 36
11. Ответственность 37
12. Разрешение споров (диспутов) 42
13. Конфиденциальность 43

1. Общие положения

Настоящие Правила национальной платежной системы «HUMO» (далее - Правила) определяют порядок организации и функционирования Национальной платежной системы «HUMO» (далее – Система), регламентируют условия участия Участников в Системе, взаимодействия ПО с Оператором, порядок информационно-технологического и финансового взаимодействия в рамках Системы, а также определяют права, обязанности и функции Участников, Расчетного центра и ПО.

1.1. Введение

Национальная платежная система «HUMO» - совокупность отношений, обеспечивающих осуществление платежей путем взаимодействия Оператора, Участников и ПО посредством применения процедур, инфраструктуры и настоящих Правил.

Целью организации Системы является обеспечение бесперебойности, эффективности и доступности оказания Участниками и ПО услуг с использованием инфраструктуры Системы в пределах предоставленных им полномочий и функциональных возможностей в соответствии с настоящими Правилами и Нормативными документами Системы.

Правила разработаны в соответствии с требованиями Законов «О платежах и платежных системах», «Об электронных платежах» и иных нормативно-правовых актов Республики Узбекистан.

Правила являются неотъемлемой частью договора об участии в Системе (обслуживании в процессинговом центре), заключаемого между Оператором и Участником, а также соглашения о взаимодействии, заключаемого между Оператором и ПО.

Правила, Тарифы и Нормативные документы Системы, являются публично доступными и размещаются на Информационном ресурсе Системы.

Оператор вправе в одностороннем порядке вносить изменения и дополнения в Правила, Тарифы и (или) Нормативные документы Системы. Оператор уведомляет Участников и ПО об изменениях в Правила, Тарифы и (или) Нормативные документы Системы путем размещения соответствующего уведомления на Информационном ресурсе Системы в течение 3 (трех) рабочих дней после их утверждения Оператором.

Изменения и дополнения в Правила, Тарифы и (или) Нормативные документы Системы применяются Оператором, Участниками и ПО через 15 (пятнадцать) календарных дней после их опубликования на Информационном ресурсе Системы.

Оператор оставляет за собой право использовать также иные доступные средства информирования Участников и ПО.

1.2. Термины и определения:

PCI DSS (Payment Card Industry Data Security Standard)	стандарт безопасности данных индустрии платежных карт, разработанный Советом по стандартам безопасности данных индустрии платежных карт. Описывает требования к защите данных о Держателях Карт при их обработке, передаче и хранении, а также, регламентирует правила безопасной разработки, поддержки и эксплуатации платежных систем.
CVV	трехзначный код проверки подлинности Карты. Может наноситься на полосу для подписи Держателя Карты. Используется в качестве защитного элемента при проведении Операций без

	предъявления Карты.
Авторизационный запрос	запрос Эквайера на получение Авторизации.
Авторизация	разрешение, предоставляемое Оператором и/или Эмитентом на проведение Операции, которое является основанием для получения Эквайером от Эмитента возмещения по Операции в размере суммы, на которую была предоставлена Авторизация.
Банкомат	устройство, предназначенное для осуществления Операций выдачи или приема наличных денежных средств с использованием Карт, иных Операций в соответствии с настоящими Правилами, и передачи распоряжений Эмитенту о переводе денежных средств со счета Клиента, а также для составления документов, подтверждающих соответствующие Операции.
БИН (банковский идентификационный номер)	6-значный цифровой идентификатор, предоставляемый Оператором Эмитенту, определяющий виды карточных продуктов Эмитента.
Держатель Карты	физическое лицо, в качестве Клиента использующее Карту на основании договора с Эмитентом, или физическое лицо - уполномоченный представитель Клиента.
Диспут	спорная ситуация, возникшая в связи с осуществлением Операции в Системе, при которой Участник и (или) ПО оспаривает правомерность, корректность, объём, сумму, сроки либо иные условия совершённой Операции и инициирует процедуру её рассмотрения, сопровождения и урегулирования в порядке, установленном Оператором.
Информационный ресурс Системы	официальный сайт Оператора по адресу www.humocard.uz, информационная система, предоставляющая доступ Участнику и (или) ПО к различным материалам и сервисам Системы.
Инцидент	событие, повлекшее или способное повлечь нарушение установленного порядка функционирования Системы и/или требований безопасности и защиты информации.
Карта	банковская карта, эмитированная Участником в рамках Системы, которое содержит информацию, позволяющую ее держателю посредством Терминалов, Банкоматов или ЭСП осуществлять платежи или получать наличные денежные средства либо производить обмен валют и другие Операции,

	определенные Участником эмитировавший Карту и на его условиях.
Клиент	физическое или юридическое лицо, которому Участником и (или) ПО оказываются услуги с использованием инфраструктуры Системы на основании соответствующего договора, в том числе лицо, которому Эмитентом выпущена Карта для совершения Операций в рамках Системы.
Код категории ТСП (Merchant Category Code, MCC)	код категории Торгово-сервисного предприятия (ТСП), присваиваемый Эквайером в соответствии с классификацией их деятельности.
Комиссия Оператора	плата, взымаемая Оператором с Участника и (или) ПО за оказание услуг в рамках Системы в соответствии с Тарифами.
Логотип	графический знак, изображение, эмблема или символ, используемый Участниками и ПО для размещения в ЭСП, на Картах, для обозначения устройств, предназначенных для совершения Операций с использованием Карт, для информирования Держателей Карт о месторасположении указанных устройств, для изготовления рекламной продукции.
Нормативные документы Системы	совокупность нормативных документов Системы, включая, но не ограничиваясь, правилами, стандартами, техническими спецификациями, регламентами, операционными бюллетенями (инструкциями), методическими рекомендациями, руководствами по продуктам и услугам, требованиями по безопасности и иными обязательными для выполнения документами, опубликованными на Информационном ресурсе Системы в действующей редакции, а также любыми их изменениями и дополнениями.
Оператор (Оператор Системы)	АО «Национальный межбанковский процессинговый центр», который определяет Правила Системы и осуществляет контроль за их соблюдением Участниками и ПО, обеспечивает функционирование Системы, информационно-технологическое взаимодействие Участников, ПО и Расчетного центра, а также доступ Участников, ПО и их Клиентов к соответствующим услугам и сервисам Системы в пределах функциональных возможностей, предусмотренных настоящими Правилами, Нормативными документами Системы и заключенными договорами, и осуществляющее иные действия, связанные с функционированием Системы и информационно-коммуникационным

	взаимодействием ее Субъектов.
Операция	действие, инициированное Держателем Карты и обрабатываемое в Системе, которое в зависимости от характера подразделяется на: (a) Финансовую операцию (финансовый запрос) — действие, связанное с движением денежных средств с использованием Карты, включая оплату, перевод, выдачу наличных денежных средств, возврат и иные операции, влекущие списание или зачисление денежных средств; (b) Нефинансовую операцию (нефинансовый запрос) — действие, не связанное с движением денежных средств, включая запрос баланса, изменение ПИН-кода, сброс счетчика неправильных попыток ввода ПИН-кода, получение информации о Карте и иные информационные или сервисные действия.
Платежная организация (ПО)	платежная организация, имеющая лицензию Центрального банка Республики Узбекистан, установившая взаимодействие с Оператором в рамках Системы и принявшая обязательство соблюдать настоящие Правила и Нормативные документы Системы в части, применимой к ее деятельности.
ПИН-код Карты (ПИН, ПИН-код)	персональный идентификационный номер Карты (секретный код), используемый Держателем Карты при проведении Операции в качестве подтверждении Операции, с помощью которого производится аутентификация Держателя Карты.
Предварительная авторизация	предварительная Авторизация, выполняемая в режиме реального времени, предназначенная для проверки достаточности средств на счете Держателя Карты или резервирования необходимой суммы средств на счете Держателя Карты в качестве гарантии оплаты товаров (работ, услуг). Не является основанием для осуществления перевода денежных средств.
Расчетный центр	Межбанковская универсальная неттинговая информационная система (МУНИС), обеспечивающий исполнение распоряжений Участников посредством списания и зачисления денежных средств по Счетам Участников по взаиморасчетам в рамках Системы.
Риск	вероятность наступления события и/или обстоятельства, способного привести к нарушению бесперебойности, безопасности и/или корректности функционирования Системы, финансовым потерям

	и/или репутационному ущербу.
Сеть устройств	совокупность Терминалов, Банкоматов и иных устройств, предназначенных для совершения Операций с использованием Карт/реквизитов Карт.
Система управления рисками в Системе (СУР)	совокупность процессов, контрольных мер и ответственности Оператора, Участников и ПО, направленных на выявление, оценку, мониторинг и снижение рисков в Системе.
Субъекты Системы	Оператор, Участники, Расчетный центр и ПО.
Счет Участника (Счет)	корреспондентский счет Участника в Расчетном центре, используемый для осуществления расчетов между Участниками Системы.
Таблица БИНов	список БИНов, формируемый Оператором, определяющий маршрутизацию Авторизационных запросов при проведении Операции.
Тарифы Системы (Тарифы)	размер и порядок взимания плат за услуги, оказываемые Оператором Участникам и (или) ПО в рамках Системе.
Терминал (POS, E-POS, M-POS)	Устройство или программное обеспечение, предназначенное для совершения Операций с использованием Карт (данные Карты), а также для составления документов, подтверждающих соответствующие Операции.
Торгово-сервисное предприятие (ТСП)	организация торговли (работ, услуг), установившая договорные взаимоотношения с Эквайером в целях использования Карт Системы в качестве электронного средства платежа для расчетов за реализуемые Держателям Карт товары (работы, услуги).
Участник	банк, заключивший с Оператором договор об участии в Системе (обслуживании в процессинговом центре) и присоединившийся к Правилам.
Эквайер	Участник, осуществляющий Эквайринг.
Эквайринг	деятельность Участника по обеспечению проведения Операций и осуществлению расчетов с ТСП по Операциям, совершаемым с использованием Карт (реквизитов Карт), и/или выдачи наличных денежных средств Держателям Карт, а также иным Операциям в соответствии с настоящими Правилами.
Электронное средство платежа (ЭСП)	способ или устройство (мобильные приложения, интернет-банкинг, электронные кошельки и иные средства дистанционного взаимодействия) Участника и (или) ПО, позволяющее Клиенту с использованием технических средств,

	информационных технологий и услуг информационных систем составлять, удостоверять и передавать распоряжения на перевод денежных средств в безналичной форме, а также инициировать Финансовые и Нефинансовые операции в Системе.
Эмиссия	деятельность Участника по выдаче (выпуску) Карт, предназначенных для совершения Операций Держателями Карт.
Эмитент	Участник, осуществляющий Эмиссию.

1.3. Обязательность Правил и их применение

Настоящие Правила являются обязательными для Оператора и Участников Системы. Для ПО Правила являются обязательными в части, применимой к осуществляемой ими деятельности, с момента установления взаимодействия с Оператором на основании соглашения о взаимодействии и присоединения к Правилам.

Настоящие Правила регулируют отношения между Оператором и Участниками и (или) ПО, возникающие при функционировании Системы, и применяются к отношениям, возникающим в связи с функционированием Системы и использованием ее инфраструктуры.

При осуществлении деятельности в рамках Системы Участники и ПО обязаны соблюдать требования законодательства Республики Узбекистан. Все Операции, совершаемые в рамках Системы, должны соответствовать требованиям законодательства Республики Узбекистан.

В случае противоречия между положениями настоящих Правил и требованиями законодательства Республики Узбекистан применяются нормы законодательства Республики Узбекистан.

Отношения, возникающие при осуществлении Операций за пределами территории Республики Узбекистан, регулируются законодательством соответствующего государства, правилами соответствующих национальных и (или) международных платежных систем, а также условиями международных договоров, соглашений и иных документов, применимых к таким Операциям.

При осуществлении трансграничных операций либо Операций, совершаемых с использованием инфраструктуры иностранных платежных систем, наряду с настоящими Правилами применяются правила соответствующих платежных систем, условия заключенных соглашений и договоров, а также нормы применимого законодательства.

Присоединение к настоящим Правилам осуществляется исключительно путем принятия их в полном объеме, без каких-либо оговорок, исключений или изменений.

1.4. Взаимодействие Оператора с иными платежными системами

В целях обеспечения функционирования, развития и расширения возможностей Системы Оператор вправе осуществлять взаимодействие с платежными системами Республики Узбекистан, платежными системами иностранных государств и международными платежными системами в соответствии с законодательством Республики Узбекистан.

Взаимодействие осуществляется на основании договоров, соглашений, меморандумов, технических регламентов и иных документов, заключаемых Оператором с соответствующими платежными системами Республики Узбекистан, платежными системами иностранных государств и международными платежными системами.

В рамках такого взаимодействия Оператор вправе:

- обеспечивать технологическую межсистемную интеграцию платежных систем;
- организовывать обработку и маршрутизацию Операций в Системе;
- обеспечивать информационный обмен, необходимый для обработки Операций, управления

рисками и предотвращения мошенничества в рамках Системы;

– организовывать выпуск и обслуживание совместных (кобейджинговых) платежных инструментов;

– утверждать обязательные для Участников и ПО технические спецификации, регламенты, стандарты и иные документы, регулирующие особенности осуществления Операций в рамках такого взаимодействия;

– осуществлять иные формы взаимодействия, не противоречащие законодательству Республики Узбекистан.

При осуществлении Операций в рамках Системы с использованием инфраструктуры платежных систем Республики Узбекистан, платежных систем иностранных государств и международных платежных систем Участники обязаны соблюдать настоящие Правила, а также обязательные требования соответствующих платежных систем в части, не противоречащей законодательству Республики Узбекистан и настоящим Правилам.

2. Товарные знаки, знаки обслуживания, логотипы и правила их использования

Оператор является правообладателем товарных знаков и знаков обслуживания Системы, предназначенных для индивидуализации Карт и оказываемых Системой услуг/работ. Оператор самостоятельно определяет требования к дизайну Карт и стандарты для использования товарных знаков, знаков обслуживания и Логотипов Системы для обеспечения целостности, безопасности и защищенности товарных знаков, знаков обслуживания и Логотипов Системы, продуктов и услуг/работ Системы в целях обеспечения узнаваемости и признания продуктов и услуг/работ Системы как на территории Республики Узбекистан, так и за его пределами.

Участники и ПО обязаны предоставлять Оператору на согласование материалы, содержащие наименование Системы, товарные знаки, знаки обслуживания или Логотипы Системы.

Описание товарных знаков, знаков обслуживания и Логотипов Системы, а также порядок их размещения и условия использования определяются Оператором.

Участники обязаны:

– размещать товарные знаки, знаки обслуживания и Логотипы Системы на эмитируемых Картах;

– обеспечить размещение товарных знаков, знаков обслуживания и Логотипов Системы на всех устройствах, предназначенных для совершения Операций с использованием Карт, а также в местах обслуживания Держателей Карт в целях информирования Держателей Карт о возможности осуществления Операций с использованием Карт;

– предоставлять Оператору на согласование все создаваемые им самостоятельно (или по их поручению) материалы, в которых имеется ссылка или упоминается название Системы и/или используются товарные знаки, и/или знаки обслуживания, и/или Логотипы Системы;

– немедленно прекратить любое использование или размещение товарных знаков, знаков обслуживания и Логотипов Системы в случае прекращения участия в Системе.

Участники вправе, исключительно с предварительного письменного согласия Оператора:

– использовать товарные знаки, знаки обслуживания и Логотипы Системы для размещения на картах, эмитированных ими в рамках участия в других платежных системах;

– размещать на Картах товарные знаки и знаки обслуживания других платежных систем;

– размещать на Картах товарные знаки и знаки обслуживания третьих лиц (авиакомпаний, торговых сетей и т.д.).

Размещение товарных знаков (знаков обслуживания) третьих лиц (авиакомпаний, торговых сетей и т.д.) на Картах возможно только при наличии согласия/разрешения правообладателей этих товарных знаков. Оператор вправе потребовать от Участника предоставление согласия/разрешения

правообладателей товарных знаков, размещаемых на Картах Участника, а Участник обязан их предоставить в порядке и сроки, указанные в требовании Оператора. Участник несет ответственность за достоверность предоставленных сведений и документов.

В иных случаях товарные знаки, знаки обслуживания и Логотипы Системы могут быть использованы исключительно с предварительного письменного согласия Оператора, при этом отсутствие запрета не считается согласием (разрешением).

Участники и ПО обязаны прекратить использование товарных знаков, знаков обслуживания и Логотипов Системы после прекращения участия в Системе либо прекращения взаимодействия с Оператором.

Присоединяясь к Правилам, Участник или ПО предоставляет Оператору право использовать свое наименование, товарные знаки и знаки обслуживания в целях рекламы и продвижения товаров, работ, услуг Системы без взимания какой-либо платы, и в течение всего срока участия в Системе, но не превышающего срока действия прав Участника или ПО на указанные объекты интеллектуальной собственности.

Если в результате такого использования Оператором будут нарушены права третьих лиц, Участник или ПО обязуется своими силами и за свой счет оградить Оператора от всех последствий, связанных с такими нарушениями, в том числе возмещений убытков третьим лицам, права которых были нарушены.

В случае нарушения Участником или ПО прав третьих лиц на любые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, ответственность за такие нарушения несет Участник или ПО. Участник или ПО обязуется своими силами и за свой счет оградить Оператора от всех последствий, связанных с такими нарушениями, в том числе возмещений убытков третьим лицам, права которых были нарушены.

3. Взаимодействие между Оператором, Участниками и Платежными организациями

3.1. Права и обязанности Оператора

Оператор обязан:

– своевременно определять Правила и Нормативные документы Системы, организовывать и осуществлять контроль за их соблюдением Участниками и ПО;

– определять и реализовывать стратегию развития Системы;

– организовать и поддерживать СУР, включая выявление, оценку и мониторинг рисков, в порядке, предусмотренном настоящими Правилами и Нормативными документами Системы, обеспечивать бесперебойность функционирования Системы в соответствии с требованиями законодательства Республики Узбекистан;

– обеспечивать бесперебойность оказания услуг платежной инфраструктуры в онлайн режиме, а также информировать Участников и ПО о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления;

– обеспечивать возможность досудебного рассмотрения споров с Участниками и ПО в соответствии с Нормативными документами Системы;

– обеспечивать равный и открытый доступ Участников к оказываемым им услугам в Системе и доступ ПО к функциональным возможностям Системы в пределах, определенных Оператором;

– обеспечивать прием, обработку и маршрутизацию файлов о совершенных транзакциях (клиринговых файлов), поступающих от Участников, в порядке и на условиях, предусмотренных настоящими Правилами и иными Нормативными документами Системы, независимо от даты/периода формирования файлов и совершения Операций, содержащихся в таких файлах, если иное не предусмотрено законодательством Республики Узбекистан, настоящими Правилами либо Нормативными документами Системы;

– обеспечивать сохранение банковской тайны, защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Республики Узбекистан;

– размещать Правила, Тарифы и Нормативные документы Системы на официальном сайте Оператора.

Оператор имеет право:

– вносить изменения и дополнения в Правила, Тарифы и Нормативные документы Системы;

– изменять условия функционирования Системы;

– запрашивать информацию о деятельности Участников и ПО в рамках Системы и требовать ее предоставления в надлежащие сроки;

– осуществлять мониторинг и выявление подозрительных Операций с использованием ЭСП в целях обеспечения безопасности денежных средств Клиента, предотвращения несанкционированных и диспутных Операций, а также управления операционными рисками;

– осуществлять изменение ПИН-кода Карты и сброс счетчика неправильных попыток ввода ПИН-кода по запросу Держателя Карты, направленному посредством ЭСП, в порядке, предусмотренном настоящими Правилами и Нормативными документами Системы, а также принимать решения о предоставлении отдельным ПО права обеспечивать изменение ПИН-кода Карты посредством предоставляемых ими ЭСП;

– осуществлять контроль за соблюдением Участниками и ПО настоящих Правил и Нормативных документов Системы, в пределах их обязанностей и ответственности, закрепленных в Правилах, в том числе за использованием товарных знаков, знаков обслуживания и Логотипов Системы;

– временно приостановить проведение Операций с использованием ЭСП, также включая блокировку Карты, Терминала, Банкомата, и другие устройства самообслуживания до выяснения обстоятельств и подтверждения Клиентом (в режиме звонка и (или) SMS) правомерности таких Операций с последующим уведомлением Клиента, Участника или ПО о причинах и совершённых действиях;

– временно приостанавливать обработку в Системе Операций, совершаемых с использованием Карт, эмитированных одним или несколькими Участниками, при наличии оснований и в порядке, предусмотренных настоящими Правилами и Нормативными документами Системы, с уведомлением соответствующих Участников о причинах принятого решения;

– направить Участнику или ПО обязательные для исполнения требования (предписания) о приостановлении, ограничении либо блокировке Карт, карточных счетов, иных ЭСП, Операций либо иных платежных инструментов в сроки, определенные Оператором;

– устанавливать минимальный размер положительного остатка денежных средств на Карте, который должен сохраняться у Клиента - физического лица при осуществлении безакцептного списания денежных средств. Указанный размер определяется исходя из совокупного остатка денежных средств на всех карточных счетах физического лица, к которым эмитированы Карты Участниками Системы. Размер минимального положительного остатка, а также его изменение устанавливаются Оператором и доводятся до сведения Участников путем направления соответствующего уведомления;

– запросить у Эквайера результаты комплексной проверки ТСП до заключения договора на Эквайринг, включая копии учредительных документов ТСП, разрешений регулирующих органов, лицензий (если применимо) и другую справочную и/или операционную информацию;

– осуществлять контроль корректности установленного Эквайером MCC-кода, а также требовать его изменения, в случае выявления несоответствия фактически осуществляемой

деятельности;

– отменять в безакцептном порядке ошибочно проведенную Операцию по зачислению или списанию денежных средств либо, если отмена такой Операции технически невозможна, осуществлять соответствующую корректировочную Операцию независимо от даты совершения первоначальной Операции и момента выявления ошибки, если иное не предусмотрено законодательством Республики Узбекистан;

– организовывать обмен информацией между Участниками и ПО о признаках подозрительной (мошеннической) активности в целях предупреждения, выявления и минимизации рисков совершения несанкционированных (фрод) Операций;

– самостоятельно определять порядок, последовательность, условия и технологию обработки клиринговых файлов, поступающих от Участников, в том числе принимать решения об их обработке независимо от даты формирования, даты направления, отчетного периода либо даты совершения Операций, содержащихся в соответствующих клиринговых файлах, если иное не предусмотрено законодательством Республики Узбекистан, настоящими Правилами и Нормативными документами Системы;

– самостоятельно определять:

  – достаточность оснований для применения ограничительных мер;
  – степень риска совершаемой Операции;
  – перечень применяемых ограничений;
  – сроки действия ограничений;
  – необходимость их продления;
  – основания для снятия ограничений;
  – порядок функционирования Системы мониторинга;
  – критерии выявления подозрительных Операций.

– приостанавливать обработку клиринговых файлов, отказывать в их обработке либо запрашивать у Участников дополнительные сведения и (или) документы в случаях выявления признаков технических ошибок, дублирования Операций, нарушения форматов обмена данными, несоответствия установленным требованиям либо иных обстоятельств, препятствующих корректной обработке таких файлов;

– самостоятельно определять периодичность, количество, время, последовательность, порядок, технологию и иные параметры обработки клиринговых файлов, а также порядок их приема, проверки, обработки, повторной обработки, отклонения, приостановления обработки и формирования результатов клиринга;

– в случае повторного совершения Участником или ПО аналогичного нарушения, за которое ранее было вынесено решение о наложении штрафных санкций, и/или при неустранении такого нарушения в течение 1 (одного) месяца с даты вынесения соответствующего решения, а также при непредоставлении в адрес Оператора письменного уведомления об устранении выявленного нарушения и неоплате наложенных штрафных санкций, Оператор вправе применить к Участнику или ПО меры временного ограничения функционала в Системе.

– пользоваться иными правами, предусмотренными законодательством Республики Узбекистан, настоящими Правилами, Нормативными документами Системы и/или заключенными договорами с Участниками и соглашениями о взаимодействии с ПО.

3.2. Права и обязанности Участников

Участник осуществляет расчеты в рамках Системы с использованием Счета Участника, открытого ему в Расчетном центре.

Участник обязан:

– осуществлять свою деятельность в соответствии с Правилами Системы;

– обеспечивать выполнение требований законодательства Республики Узбекистан, настоящих Правил и Нормативных документов Системы, а также договоров, в том числе лицами, привлеченными Участниками для оказания услуг в рамках Системы;

– незамедлительно исполнять обязательные для исполнения требования (предписания) Оператора о приостановлении, ограничении либо блокировке Карт, карточных счетов, иных ЭСП, Операций, либо иных платежных инструментов в сроки, определенные Оператором;

– при направлении Оператору запроса на изменение ПИН-кода Карты обеспечить идентификацию и двухфакторную аутентификацию Держателя Карты, одним из обязательных факторов которой является биометрическая идентификация по изображению лица (Face ID), и нести ответственность за достоверность, правомерность и корректность передаваемого Оператору запроса;

– обеспечивать своевременное формирование и направление Оператору файлов о совершенных транзакциях (клиринговых файлов) в соответствии с требованиями настоящих Правил, технологических регламентов и иных Нормативных документов Системы;

– нести полную ответственность за законность, правомерность, достоверность, полноту, актуальность, корректность и обоснованность сведений, содержащихся в направляемых Оператору клиринговых файлах, независимо от даты совершения Операций, даты формирования, направления либо обработки таких файлов Оператором;

– нести полную ответственность за направление клиринговых файлов, содержащих сведения об Операциях, совершенных в предыдущие расчетные периоды, а также за все правовые, финансовые, операционные и иные последствия, связанные с их направлением, обработкой и отражением в расчетах между Участниками Системы;

– самостоятельно урегулировать с другими Участниками Системы все разногласия, споры и претензии, связанные с содержанием клиринговых файлов, отраженными в них Операциями, суммами взаиморасчетов, корректностью переданных сведений, сроками направления файлов и иными обстоятельствами, возникающими вследствие формирования и направления таких файлов;

– по требованию Оператора незамедлительно предоставлять документы, сведения, пояснения, расчеты, выписки, копии первичных учетных документов, электронные документы, а также иные материалы и информацию, подтверждающие законность, обоснованность, достоверность и корректность сведений, содержащихся в направленных клиринговых файлах. В случае невозможности оперативного предоставления оригиналов документов или документов, оформленных в установленном порядке, Участник вправе первоначально направить Оператору их электронные копии (сканированные копии), копии, заверенные электронной цифровой подписью, либо иные документы и сведения посредством электронной почты, информационных систем, электронного документооборота или иных согласованных с Оператором каналов связи с последующим предоставлением оригиналов либо надлежащим образом оформленных документов в сроки, согласованные с Оператором;

– своевременно оплачивать услуги, оказываемые ему в рамках Системы, вознаграждение другим Участникам и осуществлять иные платежи, установленные Правилами и Тарифами Системы в порядке, определенном Правилами и Тарифами Системы;

– обеспечивать защиту информации при выполнении Операций по Картам в соответствии с требованиями Правил, Нормативных документов Системы, законодательства Республики Узбекистан и международных стандартов безопасности (PCI DSS);

– соблюдать требования СУР, предусмотренные настоящими Правилами и Нормативными документами Системы;

– предоставлять Оператору информацию, необходимую для мониторинга рисков Системы, в порядке и сроки, установленные Нормативными документами Системы;

– незамедлительно уведомлять Оператора обо всех выявленных случаях компрометации ЭСП, выявлении дроп-карт, незаконной игорной деятельности и иных событиях, способных повлиять на безопасность Системы;

– исполнять обязательные требования Оператора, направленные в соответствии с настоящими Правилами и Нормативными документами Системы, в том числе содержащиеся в уведомлениях Оператора, в порядке и сроки, указанные в таких требованиях (уведомлениях);

– предоставлять документы, сведения и пояснения по запросу Оператора не позднее 3 (трех) рабочих дней либо в иной срок, указанный (установленный) Оператором;

– оказывать содействие расследованию Операций, связанных с незаконной игорной деятельностью и иных Операций повышенного риска;

– обеспечивать сохранность доказательственной базы;

– принимать меры по предотвращению повторного совершения аналогичных инцидентов;

– незамедлительно информировать Оператора об Инцидентах и событиях, влияющих или способных повлиять на бесперебойность/безопасность Системы;

– осуществлять обслуживание Карт Участников в своей Сети устройств на условиях, установленных Правилами, Нормативными документами и Тарифами Системы;

– обеспечить выполнение требований, установленных настоящими Правилами и Нормативными документами Системы при изготовлении и Эмиссии Карт;

– отвечать перед Участниками по всем обязательствам, вытекающим из Операций, совершенных с использованием Карт и устройств Участника;

– оказывать полное содействие Оператору в расследовании диспутных и (или) несанкционированных Операций и предоставлять требуемую информацию по запросу, полученного с адресов электронной почты (cybersecurity@nmpc.uz, dispute@nmpc.uz), если иной адрес не предоставлен Оператором;

– предоставлять Оператору актуальные контактные данные своих сотрудников (ФИО, адрес корпоративной электронной почты и служебный телефон (при наличии) уполномоченных для взаимодействия по вопросам несанкционированных и (или) диспутных Операций;

– нести полную ответственность за действия/бездействия работников Участника, а также персонала сторонних организаций, привлекаемых Участником для исполнения своих обязанностей при осуществлении деятельности в Системе;

– оказывать Оператору содействие в расследовании спорных ситуаций;

– своевременно уведомлять Оператора об изменениях организационно-правовой формы, реорганизации, изменении своего места нахождения и почтового адреса, изменении своих банковских реквизитов, а также о любых других изменениях, которые могут существенным образом отразиться на исполнении Участником своих обязательств, вытекающих из Правил, включая факты банкротства и лишения лицензии на осуществление банковской деятельности и др.;

– содействовать развитию Системы;

– обеспечивать выполнение иных обязанностей, установленных Правилами, Нормативными документами Системы, заключенными договорами с Участниками.

Участник имеет право:

– выпускать Карты с товарными знаками, знаками обслуживания и Логотипами Системы собственного (индивидуального) дизайна под БИНами, предоставленными Оператором Участнику;

– иметь возможность эквайрингового обслуживания в Сети устройств Системы по всем Картам, эмитированным им в рамках участия в Системе, на условиях, установленных Правилами, Нормативными документами и Тарифами Системы;

– вносить предложения по улучшению работы Системы, введению новых услуг в рамках Системы и другим вопросам деятельности Системы;

– обжаловать применимые Оператором штрафные санкции или иные меры ограничения функционала в Системе;

– пользоваться иными правами, предусмотренными настоящими Правилами и Нормативными документами Системы, заключенными договорами с Участниками и законодательством Республики Узбекистан.

3.3. Права и обязанности Платежной организации

ПО осуществляет взаимодействие с Оператором и оказывает платежные услуги с использованием инфраструктуры Системы на основании лицензии Центрального банка Республики Узбекистан, соглашения о взаимодействии с Оператором, настоящих Правил и Нормативных документов Системы.

ПО обязана:

– осуществлять деятельность исключительно в пределах имеющейся лицензии, условий соглашения о взаимодействии с Оператором и функциональных возможностей, предоставленных ей в рамках Системы;

– соблюдать требования законодательства Республики Узбекистан, настоящих Правил, Нормативных документов Системы и соглашения о взаимодействии с Оператором;

– обеспечивать соответствие своих информационных систем, ЭСП, программного обеспечения и каналов взаимодействия техническим требованиям Оператора;

– обеспечивать законность, достоверность, полноту, актуальность и корректность направляемых Оператору запросов, электронных сообщений, документов и иных сведений;

– обеспечивать надлежащую идентификацию и аутентификацию Клиентов и Держателей Карт в случаях, предусмотренных законодательством Республики Узбекистан, настоящими Правилами и Нормативными документами Системы;

– при предоставлении посредством ЭСП возможности изменения ПИН-кода Карты по решению Оператора или сброса счетчика неправильных попыток ввода ПИН-кода обеспечивать идентификацию и двухфакторную аутентификацию Держателя Карты, получение необходимых согласий, а также передачу Оператору соответствующего запроса и сведений о его подтверждении;

– обеспечивать наличие законных оснований для сбора, обработки, хранения и передачи Оператору персональных данных, банковской тайны и иной охраняемой законом информации;

– обеспечивать защиту информации, информационную безопасность и кибербезопасность используемых информационных систем, ЭСП и каналов взаимодействия в соответствии с законодательством Республики Узбекистан, настоящими Правилами, Нормативными документами Системы и требованиями PCI DSS в применимой части;

– соблюдать требования СУР, антифрод-мониторинга и иных систем контроля, функционирующих в Системе;

– незамедлительно уведомлять Оператора о выявленных Инцидентах, случаях компрометации ЭСП или реквизитов Карт, подозрительных и несанкционированных Операциях, незаконной игорной деятельности, сбоях и иных обстоятельствах, влияющих или способных повлиять на безопасность и бесперебойность функционирования Системы;

– в пределах выполняемых функций и имеющихся технических возможностей незамедлительно исполнять обязательные требования и уведомления Оператора об ограничении или приостановлении операций, блокировке либо ограничении использования ЭСП, предоставлении информации, проведении антифрод-мероприятий и принятии иных мер безопасности;

– по запросу Оператора предоставлять документы, сведения, журналы событий, технические

данные и пояснения не позднее трех рабочих дней либо в иной срок, указанный Оператором с учетом характера и срочности запроса;

– оказывать Оператору содействие в расследовании Инцидентов, подозрительных, несанкционированных и диспутных Операций, а также сохранять сведения и материалы, имеющие значение для их рассмотрения;

– обеспечивать хранение электронных документов, подтверждений, журналов событий и иных сведений, связанных с осуществлением деятельности в Системе, в порядке и сроки, установленные законодательством Республики Узбекистан, настоящими Правилами и Нормативными документами Системы;

– самостоятельно рассматривать и урегулировать обращения Клиентов, связанные с услугами ПО, функционированием предоставляемых ею ЭСП, идентификацией и аутентификацией Клиентов, а также действиями или бездействием ПО;

– обеспечивать соблюдение привлеченными третьими лицами требований законодательства Республики Узбекистан, настоящих Правил, Нормативных документов Системы и соглашения о взаимодействии с Оператором и нести ответственность за их действия или бездействие в пределах, предусмотренных законодательством и соглашением о взаимодействии;

– предоставлять Оператору актуальные контактные данные работников, уполномоченных на взаимодействие по операционным, техническим, антифрод-вопросам, вопросам информационной безопасности и урегулирования диспутов;

– незамедлительно уведомлять Оператора об изменении наименования, организационно-правовой формы, места нахождения, банковских реквизитов, реорганизации, ликвидации, банкротстве, а также о приостановлении, ограничении или отзыве лицензии и иных обстоятельствах, способных повлиять на исполнение обязательств ПО;

– использовать товарные знаки, знаки обслуживания и Логотипы Системы исключительно в порядке и на условиях, установленных настоящими Правилами, Нормативными документами Системы и письменным согласованием Оператора;

– соблюдать конфиденциальность информации, полученной в связи с осуществлением деятельности в Системе;

– своевременно вносить плату в рамках взаимодействия с Оператором и исполнять иные финансовые обязательства в порядке и сроки, предусмотренные соглашением о взаимодействии и применимыми Тарифами;

– выполнять иные обязанности, предусмотренные законодательством Республики Узбекистан, настоящими Правилами, Нормативными документами Системы и соглашением о взаимодействии с Оператором.

ПО вправе:

– оказывать Клиентам платежные услуги с использованием инфраструктуры и сервисов Системы в пределах имеющейся лицензии и условий соглашения о взаимодействии с Оператором;

– получать доступ к информационным ресурсам, сервисам и технической инфраструктуре Системы в объеме и порядке, предусмотренных соглашением о взаимодействии с Оператором и Нормативными документами Системы;

– получать от Оператора информацию, технические спецификации, регламенты, уведомления и иные документы, необходимые для осуществления взаимодействия в рамках Системы;

– обращаться к Оператору за разъяснениями и технической поддержкой по вопросам функционирования Системы и использования предоставленных сервисов;

– направлять Оператору предложения по совершенствованию Системы, развитию сервисов

и улучшению порядка взаимодействия;

– использовать товарные знаки, знаки обслуживания и Логотипы Системы в порядке и на условиях, установленных настоящими Правилами и письменным согласованием Оператора;

– представлять письменные объяснения и возражения, а также обжаловать примененные Оператором меры воздействия и штрафные санкции в порядке, предусмотренном настоящими Правилами и Нормативными документами Системы;

– прекратить взаимодействие с Оператором в порядке и на условиях, предусмотренных соглашением о взаимодействии и настоящими Правилами;

– пользоваться иными правами, предусмотренными законодательством Республики Узбекистан, настоящими Правилами, Нормативными документами Системы и соглашением о взаимодействии с Оператором.

3.4. Приобретение статуса ПО не означает приобретения статуса Участника, Эмитента или Эквайера. Положения настоящих Правил, регулирующие эмиссию Карт, эквайринг, предоставление и использование БИНов, ведение Счета Участника, клиринг и расчеты между Участниками, не распространяются на ПО, если иное прямо не предусмотрено законодательством Республики Узбекистан и соответствующим соглашением о взаимодействии.

3.5. Приостановление или прекращение взаимодействия ПО с Оператором не освобождает ПО от исполнения ранее возникших финансовых обязательств, ответственности за допущенные нарушения, а также обязанностей по обеспечению конфиденциальности, хранению информации и урегулированию поступивших обращений и требований.

4. Порядок ведения перечня Участников

Оператор ведет перечень Участников и размещает информацию об Участниках на Информационном ресурсе Системы.

Перечень включает в себя следующую информацию по каждому Участнику:

– наименование Участника;

– место нахождения (адрес) Участника;

– контактный телефон и адрес официального сайта Участника.

5. Процедуры вступления и выхода из Системы

5.1. Порядок вступления Участника в Систему

Участник присоединяется к Правилам путем подписания с Оператором соответствующего договора на оказание услуг процессинга в рамках платежной системы «HUMO». Присоединение к Правилам означает принятие Участником Правил в целом без каких-либо изъятий или ограничений.

Взаимодействие ПО с Оператором начинается с даты, определенной соответствующим соглашением о взаимодействии, и может быть приостановлено или прекращено в случаях, предусмотренных соглашением о взаимодействии, настоящими Правилами и Нормативными документами Системы, включая приостановление или отзыв лицензии ПО.

5.2. Порядок приостановления и прекращения участия Участника в Системе

Прекращение и приостановление участия в Системе возможно по следующим основаниям:

– по инициативе Участника;

– по инициативе Оператора;

– по соглашению сторон;

– в иных случаях, предусмотренных Правилами, Нормативными документами Системы и законодательством Республики Узбекистан.

Прекращение участия в Системе по инициативе Участника.

Участник может в одностороннем порядке принять решение о прекращении участия в Системе. В случае принятия такого решения Участник должен направить Оператору Заявление о прекращении участия.

В Заявлении о прекращении участия должна быть указана дата, после которой Участник обязан прекратить все осуществляемые в рамках Системы Операции по Картам и в Сети устройств Участника.

После получения Оператором Заявления о прекращении участия в Системе с указанной в заявлении даты прекращения участия Оператор предпринимает меры по блокировке БИНов Участника и прекращению обработки Операций по Картам и в Сети устройств Участника.

Участник обязан до даты прекращения участия:

– исполнить все финансовые и иные обязательства, возникшие у Участника перед всеми Участниками за период деятельности в Системе в качестве ее Участника;

– передать Оператору всю конфиденциальную информацию в соответствии с Правилами;

– удалить наклейки и информационные материалы с товарными знаками, знаками обслуживания и Логотипами Системы со всех обслуживаемых Участником Банкоматов, устройств самообслуживания, Терминалов и иных устройств, предназначенных для совершения Операций, а также с указателей, предназначенных для информирования Держателей Карт о месторасположении указанных устройств, не позднее 10 (десяти) рабочих дней, следующих за датой прекращения участия.

Участие в Системе полностью прекращается не ранее чем по истечении 90 (девяноста) календарных дней со дня проведения последней Операции по Картам или в Сети устройств Участника при условии отсутствия у Участника неисполненных финансовых обязательств перед другими Участниками, возникших в связи с Операциями и взаиморасчетами, осуществленными в рамках Системы.

После окончания указанного выше срока урегулирования обязательств Оператор письменно уведомляет Расчетный центр о факте прекращения участия в Системе данного Участника в добровольном порядке и отсутствии у него финансовых обязательств. Расчетный центр осуществляет соответствующие процедуры прекращения участия в Системе согласно своим внутренним регламентам.

Прекращение участия в Системе не освобождает Участника от обязательств и ответственности, возникших в рамках его деятельности в Системе.

Приостановление и прекращение участия по инициативе Оператора.

Участие может быть приостановлено Оператором в случаях нарушения Участником требований Правил Системы, а также, если Участник не способен выполнять свои обязательства как Участника, в том числе, но не ограничиваясь:

– неисполнения или ненадлежащего исполнения Участником своих обязательств перед Участниками;

– нанесения вреда деловой репутации Системы;

– невозможности удовлетворения предъявленных к Счету Участника в Расчетном центре требований для осуществления расчетов по Операциям, в том числе по причине наложения ареста на денежные средства на Счете, приостановления Операций по Счету в соответствии с законодательством Республики Узбекистан;

– неосуществления Участником всех необходимых мер в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма;

– выявления негативных факторов, влекущих риски нарушения Участником бесперебойности функционирования Системы;

– выявления влияющих на безопасность функционирования Системы нарушений Участником требований к обеспечению защиты информации в Системе;

– неисполнение Участником требований СУР в Системе;

– отсутствие Операций у Участника в течение 6 (шести) календарных месяцев подряд.

В случае принятия Оператором решения о приостановлении участия в Системе Оператор направляет Участнику уведомление о приостановлении его участия в Системе с указанием нарушения, послужившего причиной принятия Оператором решения, в котором также определяется срок, в течение которого нарушение должно быть устранено.

Деятельность Участника в Системе возобновляется при условии устранения нарушения, указанного Оператором в уведомлении.

Если нарушение не будет устранено в установленный срок, Оператор вправе инициировать процедуру прекращения участия Участника в Системе.

После принятия решения о прекращении участия Оператор направляет уведомление Участнику, содержащее основания и дату прекращения его участия.

Оператор предпринимает меры по блокировке БИНов Участника и прекращению обработки Операций по Картам и в Сети устройств Участника.

В период с даты направления Оператором уведомления о прекращении участия в Системе до даты прекращения участия в Системе Участник обязан:

– исполнить все финансовые и иные обязательства, возникшие у Участника перед всеми Участниками за период деятельности в Системе в качестве ее Участника;

– передать Оператору всю конфиденциальную информацию в соответствии с Правилами;

– удалить наклейки и информационные материалы с товарными знаками, знаками обслуживания и Логотипами Системы со всех обслуживаемых Участником Банкоматов, устройств самообслуживания, Терминалов и иных ЭСП, предназначенных для совершения Операций, а также с указателей, предназначенных для информирования Держателей Карт о месторасположении указанных устройств, не позднее 10 (десяти) рабочих дней с даты получения Участником уведомления о прекращении участия.

Участие в Системе полностью прекращается не ранее чем по истечении 90 (девяноста) календарных дней со дня проведения последней Операции по Картам или в Сети устройств Участника при условии отсутствия у Участника неисполненных финансовых обязательств перед другими Участниками, возникших в связи с Операциями и взаиморасчетами, осуществленными в рамках Системы.

После окончания указанного выше срока урегулирования обязательств Оператор письменно уведомляет Расчетный центр о факте прекращения участия в Системе данного Участника и отсутствии у него финансовых обязательств;

Прекращение участия в Системе не освобождает Участника от обязательств, возникших в рамках его деятельности в Системе.

Безоговорочными условиями прекращения участия в Системе являются:

– отзыв у Участника лицензии на осуществление банковской деятельности;

– признание Участника банкротом (несостоятельным);

– в иных случаях, предусмотренных законодательством Республики Узбекистан.

Приостановление и прекращение участия по соглашению сторон

Оператор и Участник могут подписать соглашение, в котором указывается дата приостановления или прекращения участия Участника в Системе, после которой Участник обязан прекратить все осуществляемые в рамках Системы Операции по Картам и в Сети устройств Участника.

Участник обязан до даты прекращения участия:

– исполнить все финансовые и иные обязательства, возникшие у Участника перед всеми Участниками за период деятельности в Системе в качестве ее Участника;

– передать Оператору всю конфиденциальную информацию в соответствии с Правилами;

– удалить наклейки и информационные материалы с товарными знаками, знаками обслуживания и Логотипами Системы со всех обслуживаемых Участником Банкоматов, устройств самообслуживания, Терминалов и иных устройств, предназначенных для совершения Операций, а также с указателей, предназначенных для информирования Держателей Карт о месторасположении указанных устройств, не позднее 10 (десяти) рабочих дней, следующих за датой прекращения участия.

Участие в Системе полностью прекращается не ранее чем по истечении 90 (девяноста) календарных дней со дня проведения последней Операции по Картам или в Сети устройств Участника при условии отсутствия у Участника неисполненных финансовых обязательств перед другими Участниками, возникших в связи с Операциями и взаиморасчетами, осуществленными в рамках Системы.

После окончания, указанного выше срока урегулирования обязательств Оператор письменно уведомляет Расчетный центр о факте прекращения участия в Системе данного Участника по соглашению сторон и отсутствии у него финансовых обязательств. Расчетный центр осуществляет соответствующие процедуры согласно своим внутренним регламентам.

Прекращение участия в Системе не освобождает Участника от обязательств и ответственности, возникших в рамках его деятельности в Системе.

6. Эмиссионная деятельность

6.1. Права и обязанности Эмитента

Эмитент в Системе выполняет следующие функции:

– осуществляет Эмиссию Карт с товарными знаками, знаками обслуживания и Логотипами Системы, в соответствии с требованиями, определяемыми настоящими Правилами и Нормативными документами Системы;

– обеспечивает осуществление расчетов с Клиентами по Операциям Держателей Карт, полученных от Оператора;

– обеспечивает осуществление расчетов с Эквайерами по Операциям с использованием Карт Эмитента в Сети устройств Эквайеров;

– обеспечивает безопасность процессов Эмиссии Карт;

– разрабатывает правила использования Карт Эмитента, определяет меру возмещения при утере (или порче) или несанкционированном использовании Держателями Карт;

– участвует в разрешении споров по Операциям, совершенным с использованием Карт Эмитента в Сети устройств Эквайеров.

Эмитент обязан:

– осуществлять деятельность в соответствии с требованиями настоящих Правил и Нормативных документов Системы;

– использовать для Эмиссии Карт только БИНы, предоставленные Участнику Оператором;

– при выпуске Карты Эмитент направляет Оператору запрос на установку ПИН-кода Карты в порядке, установленном Правилами и Нормативными документами Системы. Оператор осуществляет установку ПИН-кода Карты на основании полученного от Эмитента запроса;

– согласовывать с Оператором дизайн Карт в порядке, предусмотренном Нормативными документами Системы;

– соответствовать требованиям по безопасности, предъявляемым Системой к хранению, перемещению и уничтожению Карт;

– иметь в своем штате квалифицированный персонал, который будет непосредственно отвечать за все аспекты безопасности Карт, а также обязан:

– осуществлять мониторинг Операций с использованием Карт с целью выявления случаев их незаконного использования;

– расследовать случаи незаконного использования Карт;

– планировать и контролировать производство, персонализацию, кодирование, печать и прочие процедуры, связанные с эмиссией Карт.

– в случае соблюдения Эквайером настоящих Правил и Нормативных документов Системы обеспечить Эквайерам возмещение по Операциям с Картами Эмитента в сумме подтвержденной Авторизации;

– по запросу Оператора предоставлять сведения статистического характера об Операциях, совершенных в Сети устройств с использованием Карт Эмитента;

– предоставлять Держателям Карт полную информацию обо всех Операциях, совершённых с использованием ЭСП или иных платежных инструментов Системы способом, предусмотренным в договоре;

– предоставлять Держателям Карт полную информацию о правилах обслуживания Карт в Системе, консультировать по правилам использования Карт Эмитента;

– организовать круглосуточную поддержку Держателей Карт для оказания помощи при использовании ими Карт;

– оказывать содействие в решении проблем Держателей Карт, возникших при совершении Операций в Сети устройств Системы;

– обеспечивать возможность оперативной блокировки Карт, ограничения Операций и исполнения antifraud-требований Оператора, включая исполнение требований, связанных с предотвращением мошеннических Операций и блокировкой цепочек переводов денежных средств;

– При наличии собственного аппаратно-программного комплекса:

- информировать Оператора о плановой приостановке более чем на 1 час своего аппаратно-программного комплекса за 5 (Пять) рабочих дней до приостановки;
- соответствовать требованиям стандартов безопасности PCI DSS.

Эмитент имеет право:

– эмитировать Карты с товарными знаками, знаками обслуживания и Логотипами Системы собственного (индивидуального) дизайна под БИНами, предоставленными Оператором Эмитенту;

– самостоятельно определять финансовые взаимоотношения с Клиентами по Операциям, совершаемым с использованием Карт в Сети устройств;

– привлекать сторонние организации для исполнения своих функциональных обязанностей и обязательств, определенных Правилами и Нормативными документами Системы. Ответственность перед Участниками за деятельность указанных организаций несет Эмитент.

6.2. Порядок предоставления БИНов

Оператор может назначить Участнику БИН только после его присоединения к Системе на правах участника Системы. БИН является уникальным и не может быть использован другими Участниками.

Участник не вправе передавать право на использование БИНа, назначенного ему Оператором, другим кредитным организациям.

Для каждого типа Карт (карточных продуктов) должен быть использован отдельный БИН.

Совмещение разных видов карточных продуктов на одном БИНе не допускается.

Для получения дополнительного БИНа Участник должен направить в адрес Оператора соответствующее заявление по утвержденной форме.

Участник может отказаться от использования дополнительного БИНа путем направления в адрес Оператора соответствующего заявления по утвержденной форме. Оператор не позднее рабочего дня, следующего за днем получения такого уведомления, предпринимает меры по блокировке БИНа. Комиссия Оператора за назначение БИНа Участнику не возвращается.

6.3. Требования к договору Эмитента с Клиентом

Договор Эмитента с Клиентом определяет взаимоотношения Эмитента и его Клиента в связи с предоставлением Клиенту Карт и правила их использования.

Эмитент обязан предусмотреть в договоре с Клиентом как минимум следующие условия:

– требования по обеспечению безопасного использования Карты и ЭСП, включая:
  - недопустимость передачи Карты и ПИН-кода, OTP-кода, доступа к ЭСП для использования третьими лицами;
  - не хранить ПИН-код вместе с Картой;
  - обеспечивать защиту мобильного телефона, SIM-карты и электронной почты, а также доступа к ЭСП;
  - незамедлительно уведомлять Эмитента при утрате Карты, мобильного телефона, SIM-карты, доступа к ЭСП или подозрении на компрометацию данных.

– Карта не должна использоваться в каких-либо противозаконных целях, в том числе приобретения товаров (работ, услуг), запрещенных законодательством Республики Узбекистан;

– ответственность Клиента перед Эмитентом по оплате Операций, совершенных с использованием Карты;

– требования к порядку и срокам информирования Эмитента Держателем Карты о ставших ему известными случаях несанкционированного использования Карты, а также в случае утраты Карты;

– размер и порядок взимания с Клиента вознаграждения Эмитента;

– способы и адресаты для подачи претензий по Операциям и порядок их рассмотрения;

– условия о предоставлении Клиентом согласия на обработку его персональных данных, включая их сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу Эмитентом Оператору, а также передачу Оператором персональных данных Участникам и ПО Системы, государственным органам, правоохранительным органам, судам, Центральному банку Республики Узбекистан, иным уполномоченным государственным органам, организациям и третьим лицам в случаях и объеме, необходимых для функционирования Системы, оказания услуг, исполнения Правил и Нормативных документов Системы, обеспечения информационной безопасности, предотвращения и расследования противоправных и/или мошеннических Операций, исполнения требований законодательства Республики Узбекистан, а также защиты прав и законных интересов Участников и Клиентов. Такое согласие должно предусматривать возможность обработки персональных данных без ограничения срока до достижения целей их обработки либо до момента отзыва согласия Клиентом в случаях и порядке, предусмотренных законодательством Республики Узбекистан;

– обязанность Клиента по незамедлительному уведомлению Эмитента о выявлении денежных средств, ошибочно зачисленных на карточный счет либо отраженных в качестве доступного остатка по Карте вследствие технической ошибки, не совершать Операции с использованием указанных денежных средств и выполнять законные требования Эмитента, направленные на устранение последствий ошибочного зачисления;

– обязанность Клиента по незамедлительному уведомлению Эмитента об утрате Карты, компрометации ее реквизитов, ПИН-кода, одноразовых паролей, средств аутентификации либо о возникновении подозрений относительно совершения несанкционированных Операций;

– способы уведомления Клиента о совершении каждой Операции с использованием Карты одним или несколькими способами (SMS, Push-уведомление, электронная почта и иные способы), при этом как минимум один из способов уведомления должен предоставляться Клиенту без взимания платы;

– право Эмитента приостанавливать, ограничивать либо блокировать использование Карты, электронного средства платежа или отдельных Операций в случаях, предусмотренных законодательством Республики Узбекистан, настоящими Правилами либо договором с Клиентом;

– обязанность Клиента незамедлительно сообщать Эмитенту об изменении номера мобильного телефона, адреса электронной почты и иных контактных данных, используемых для получения уведомлений и подтверждения Операций.

Эмитент вправе принять решение о временном приостановлении Операций по Картам и изъятии Карты из обращения при наличии у него оснований, подтверждающих незаконное использование Карты или её реквизитов, а также при использовании Карты лицами, не имеющими полномочий на её использование.

Оператор не рассматривает претензии Клиентов Эмитента на недобросовестное исполнение Эмитентом условий договоров с Клиентами, но наличие таких претензий может стать причиной инициирования изучения Участника на соответствие требованиям Правил и Нормативных документов Системы.

Операция считается подтвержденной и совершенной Клиентом, если при ее проведении были использованы предусмотренные Эмитентом средства аутентификации, включая ввод ПИН-кода, OTP-кода, подтверждение в ЭСП, биометрическую аутентификацию либо иные средства подтверждения, предусмотренные Эмитентом.

7. Эквайринговая деятельность

7.1. Права и обязанности Эквайера

Эквайер выполняет в Системе следующие функции:

– обслуживает и управляет Сетью устройств, предназначенных для совершения Операций с использованием Карт;

– проводит в Сети устройств Эквайера Операции, определенные в Правилах;

– участвует в разрешении споров по Операциям, совершенным в Сети устройств Эквайера;

– обеспечивает безопасное функционирование Сети устройств.

Эквайер обязан:

– осуществлять деятельность в рамках участия в Системе в соответствии с требованиями Правил и Нормативных документов Системы;

– обеспечивать бесперебойное, равноправное обслуживание всех Карт Участников в своей Сети устройств;

– использовать для обслуживания Карт устройства и оборудование, согласованное и сертифицированное Оператором;

– обеспечить безопасность и защищенность Операций по Картам в Сети устройств Эквайера в соответствии с Правилами, Нормативными документами Системы и законодательством Республики Узбекистан;

– осуществлять мониторинг Операций и деятельности ТСП в целях своевременного выявления подозрительных, мошеннических либо противоправных Операций, а также

незамедлительно исполнять требования Оператора по ограничению либо приостановлению Операций;

– наносить товарные знаки, знаки обслуживания и Логотипы Системы на устройства, предназначенные для совершения Операций с использованием Карт, а также на указатели, предназначенные для информирования Клиентов о месторасположении устройств, предназначенных для совершения Операций с использованием Карт;

– предоставлять Держателям Карт Участников полную информацию об условиях обслуживания Карт в Сети устройств Эквайера, включая информацию о размерах дополнительной комиссии, взимаемой с Держателя Карты по тем или иным Операциям, если такое имеет место;

– поддерживать на Счете в Расчетном центре остаток денежных средств в размере, достаточном для расчета с Участниками по Операциям, совершаемым в Сети устройств Эквайера;

– предоставлять по запросу Оператора сведения статистического характера об Операциях, совершенных в Сети устройств Эквайера с использованием Карт Участников, в указанные Оператором сроки;

– привлекать ТСП при условии заключения договора с каждым ТСП;

– обеспечивать работоспособность своей Сети устройств и предусмотреть в договоре с ТСП обязательства ТСП по поддержанию работоспособности устройств;

– при подключении ТСП к обслуживанию Карт осуществлять назначение кода категории ТСП (MCC) строго в соответствии с классификацией деятельности ТСП и обеспечить указание MCC в запросах Авторизации и клиринговых сообщениях;

– иметь достаточный ресурс для своевременного и эффективного обнаружения подозрительной и мошеннической активности ТСП;

– осуществлять контроль всех Терминалов (включая виртуальные), принятых на эквайринговое обслуживание, с целью мониторинга и предотвращения подозрительной активности и (или) их несанкционированного использования;

– осуществлять контроль за деятельностью ТСП с целью мониторинга и предотвращения:

- нецелевого использования устройств обслуживания Карт, предоставленных или согласованных к использованию с Эквайером;
- использование устройств обслуживания Карт, предоставленных или согласованных к использованию с Эквайером, с целью совершения мошеннических действий;
- принятие в качестве средства оплаты за товары (работы, услуги) поддельных Карт.

– При наличии собственного аппаратного программного комплекса, подключенного к Процессингу:

- обеспечить тестовую проверку аппаратно-программного комплекса по методике и программе, согласованной с Оператором и при его участии;
- обеспечивать круглосуточную работоспособность аппаратно-программного комплекса Эквайера по сбору, обработке и хранению данных об Операциях;
- обеспечивать определенный в Системе уровень готовности аппаратно-программного комплекса Эквайера, а также устройств и оборудования, используемого для обслуживания Карт;
- соответствовать требованиям стандартов безопасности PCI DSS;
- информировать Оператора о плановой приостановке более чем на 1 час своего аппаратно-программного комплекса, обеспечивающего сбор, обработку и хранение данных об Операциях, за 3(три) рабочих дня до приостановки.

– ежеквартально в электронной форме предоставлять Оператору сведения о Сети устройств

Участника, предназначенной для обслуживания Держателей Карт;

– актуализировать МСС ТСП, если:

- изменился вид деятельности ТСП;
- выявлен мискодинг (не верная классификация деятельности ТСП);
- получено предписание Оператора.

– оказывать полное содействие Оператору в расследовании диспутных и (или) несанкционированных Операциях;

– отправить Операцию, по которой была получена успешная Авторизация, на платёжный клиринг не позднее 7 (семи) календарных дней от даты её совершения;

– до принятия на эквайринговое обслуживание проводить комплексную проверку привлекаемых ТСП, в том числе иметь копии учредительных документов ТСП, разрешений регулирующих органов, лицензий (если применимо) и другую справочную и/или операционную информацию.

Эквайер имеет право:

– привлекать сторонние организации, для исполнения своих функциональных обязанностей и обязательств, определенных Правилами. Ответственность перед Участниками за деятельность этих организаций несет Эквайер.

7.2. Взаимодействие Эквайера с ТСП

Эквайер обязан заключить с каждым обслуживаемым им ТСП отдельный договор, определяющий взаимоотношения Эквайера и ТСП, осуществляющего реализацию товаров (работ, услуг) с использованием Карт.

Эквайер несет ответственность за то, чтобы Правила Системы, в части достаточной и необходимой для осуществления деятельности по обслуживанию Карт, были доведены до ТСП и соблюдались ими.

Эквайер должен обеспечить представление интересов ТСП в процессах урегулирования споров по Операциям, совершенным ТСП с использованием Карт.

Эквайер обязан приостановить совершение Операций ТСП в случае, если деятельность данного ТСП может нанести вред репутации Системы.

Договор Эквайера с ТСП также должен включать в себя как минимум следующие положения:

– ТСП обязано соблюдать законодательство Республики Узбекистан, настоящие Правила;

– ТСП не вправе принимать к оплате Карты и осуществлять Операции с их использованием в случаях, когда такие Операции противоречат законодательству Республики Узбекистан, настоящим Правилам или условиям договора;

– ТСП не имеет права устанавливать более высокие цены при оплате Картой товаров (работ, услуг) по сравнению с оплатой иным способом или картами других платёжных систем;

– Эквайер вправе отказать в обработке Операции, приостановить расчёты с ТСП либо расторгнуть договор при выявлении признаков нарушения законодательства Республики Узбекистан и настоящих Правил;

– Эквайер имеет право на ограничение и (или) расторжение договора с ТСП по требованию Оператора;

– ТСП не вправе дискриминировать держателей платежных инструментов Системы путем установления менее благоприятных условий оплаты товаров (работ, услуг) по сравнению с покупателями, использующими иные способы оплаты;

– ТСП не вправе требовать от Клиента раскрытия ПИН-кода, одноразовых паролей, CVV-

кода и иных аутентификационных данных;

– все Операции осуществляются с обязательной авторизацией и аутентификацией (ввод ПИН-кода, OTP-кода), за исключением случаев, предусмотренных настоящими Правилами (в случае совершения Операции без надлежащей аутентификации Держателя Карты и последующему заявлению её как несанкционированной, то ответственность за риски, связанные с совершением такой Операции возлагаются на ТСП (Эквайера) в соответствии с законодательством Республики Узбекистан и Нормативными документами Системы);

– ТСП обязано передать Эквайеру задержанную Карту, по которой Эмитентом был дан соответствующий код отказа (Pick-Up Response Code), в течение 5 (Пяти) рабочих дней в соответствии
с требованиями настоящих Правил;

– ТСП обязано обеспечивать сохранность и конфиденциальность данных Держателей Карт, соблюдать требования по защите персональных данных Клиентов и информационной безопасности;

– ТСП обязано предоставлять Эквайеру требуемую информацию и документы по Операциям, необходимым для урегулирования споров (диспутов), отмены платежей и (или) проведения проверок;

– ТСП обязано незамедлительно уведомлять Эквайера о выявленных случаях подозрительных или несанкционированных Операции, компрометации данных или иных Инцидентах информационной безопасности.

7.3. Требования к оформлению и функционалу Интернет–сайта ТСП для приёма оплаты с использованием реквизитов Карт (интернет-эквайринг).

Интернет-сайт ТСП должен:

– иметь статический IP адрес;

– быть обеспечен защитой безопасным соединением протокола HTTPS, с наличием SSL/TLS - сертификата;

– иметь (и предоставить Эквайеру) подтверждение на право-обладание доменом (сайтом);

– быть зарегистрирован и располагаться в домене зоны «UZ»;

– разместить на сайте логотип Системы;

– разместить регистрационную форму для Клиента - данные о Клиенте, оформляющем заказ, контактные данные (№ телефона, электронный адрес), адрес/условия доставки товаров/оказания услуг и т.д.;

– осуществлять переход к оплате только после ознакомления и принятием Клиентом условий Оферты (акцепта) ТСП путём подтверждения на сайте;

– содержать «Публичное соглашение» или «Оферту», которая должна включать в себя:

  – описание способов заказа и оплаты;

  – условия возврата товара (отказа от услуги) отмены Операции по Карте и возврата средств на Карту;

  – условия доставки товаров/оказания услуг;

  – информацию о мерах по обеспечению безопасности Операций с использованием Карт;

  – политику конфиденциальности.

  – содержать перечень категорий товаров/услуг, который должен соответствовать информации, предоставленной при регистрации Интернет-сайта (в Анкете регистрации);

– разместить информацию о лицензиях, разрешениях от производителя, правообладателя или государственных органов на реализуемые товары/услуги, которые попадают под требование лицензирования либо наличия разрешения от правообладателя;

– не содержать и/или отображать информацию, запрещенную к распространению в соответствии с законодательством Республики Узбекистан и настоящими Правилами;

– не запрашивать на своей Интернет-странице, принимать, хранить, обрабатывать и передавать реквизиты Карт. Ввод номера Карты и других платёжных реквизитов должен осуществляться только на стороне платёжной Интернет-странице Оператора.

– не содержать неработающие страницы, ссылки, переход с которых не соответствуют их названиям, а также страниц/ссылок, перенаправляющих на другие сайты.

7.4. Требования к оформлению мест обслуживания Карт

Эквайер обязан размещать изображение товарного знака, знака обслуживания и Логотипа Системы для визуального информирования Держателей Карт о возможности приема Карт к обслуживанию на кассах, витринах и входных дверях структурных подразделений Эквайера и ТСП, с которыми Эквайер заключил договор на обслуживание Карт, на Банкоматах, интернет-сайтах и других устройствах, предназначенных для обслуживания Держателей Карт.

В случае прекращения договора с ТСП на обслуживание Карт, а также прекращении обслуживания Карт в конкретных устройствах Эквайера, наклейки с логотипом Системы должны быть удалены в срок не более 5 (пяти) рабочих дней.

7.5. Правила проверки ТСП

Перед заключением с ТСП договора на эквайринговое обслуживание, Эквайер должен провести комплексную проверку ТСП на отсутствие риска сотрудничества, законности бизнеса и кредитоспособности ТСП.

Проверка по процедуре «Знай своего клиента» (KYC):

ТСП направляет Эквайеру все необходимые документы для прохождения процедур идентификации и верификации клиентов (KYC) и комплаенс-контроля в соответствии с требованиями и внутренними правилами Эквайера. В том числе анкетные данные ТСП (Заполнение Анкеты с использованием, предусмотренной в Договоре с ТСП типовой формы Анкеты, должно быть обязательным).

ТСП предоставляет Эквайеру:

– полное юридическое наименование ТСП, сокращённое наименование ТСП, наименование ТСП в латинской транскрипции;

– регистрационные данные (ИНН, ОКЭД, ПИНФЛ (для учредителей физ. лиц);

– юридический адрес и фактический адрес/адреса ТСП (в случае наземного эквайринга) (проверка на «фирмы – однодневки»);

– в случае необходимости лицензирования деятельности – соответствующие лицензии и разрешения от уполномоченных официальных органов;

– документы собственности, аренды на торговые / складские площади;

– документы, подтверждающие полномочия лица, подписывающего документы.

Со стороны Эквайера необходим физический выезд представителя в целях проверки физического местонахождения офиса, торговых площадей, склада для проверки факта ведения ТСП реальной хозяйственной деятельности, наличия персонала и пр., а также проверки фактического соответствия реализуемых товаров/услуг – заявленным в анкете.

Проверка финансовой и деловой репутации ТСП осуществляется проверкой:

– налоговой задолженности;

– имущество, транспорт под залогом;

– признаки неплатёжеспособности;

– время работы на рынке (отзывы в Интернете);

– деловой репутации собственников, руководства.

7.6. Правила присвоения MCC-кодов

Эквайер обязан обеспечить присвоение ТСП MCC кода, наиболее точно соответствующего основному виду деятельности ТСП и реализуемым им товарам (работам, услугам).

MCC-код присваивается на основании документов и сведений, предоставленных ТСП, а также результатов проверки деятельности ТСП, проведенной Эквайером.

Не допускается присвоение ТСП MCC-кода, не соответствующего фактическому характеру деятельности ТСП, с целью обхода требований законодательства Республики Узбекистан, настоящих Правил, Тарифов, ограничений либо процедур управления рисками.

В случае изменения характера деятельности ТСП Эквайер обязан обеспечить актуализацию MCC-кода в разумный срок после получения соответствующей информации от ТСП.

Оператор вправе потребовать от Эквайера изменить MCC-код ТСП, если установленный код не соответствует фактической деятельности ТСП либо требованиям Системы.

Эквайер несёт ответственность за корректность присвоения MCC-кодов обслуживаемым ТСП и обязан по запросу Оператора предоставить обоснование присвоенного MCC-кода и подтверждающие документы.

В случае выявления некорректного MCC-кода Оператор вправе потребовать устранения нарушения, применить меры управления рисками, а также иные штрафы и (или) меры воздействия, предусмотренные настоящими Правилами.

7.7. Порядок работы с изъятыми Картами

Карта может быть изъята из обращения в случаях, предусмотренных действующим законодательством Республики Узбекистан, а также в результате технического сбоя Банкомата или устройств самообслуживания.

В случае принятия решения о приостановлении Операций и (или) изъятии Карты из обращения Эмитент в ответ на запрос Авторизации отвечает одним из двухсотых кодов отказа группы «Pick-Up», не подлежащих возврату, и незамедлительно информирует об этом Держателя карты посредством SMS-сообщения и/или иным способом уведомления, закреплённым в договоре.

В случае получения ТСП соответствующего кода отказа Эмитента, указывающего на необходимость изъятия Карты, производятся следующие действия:

– немедленно прекратить проведение Операции;

– изъять Карту у Держателя Карты;

– обеспечить сохранность Карты;

– надлежащим образом уведомить Эквайера и передать ему изъятую Карту в установленном порядке.

В случае получение в момент обслуживания Карты в Банкомате соответствующего кода отказа Эмитента, указывающего на необходимость изъятия Карты, то производится помещение Карты в специальное хранилище Банкомата до момента инкассации и дальнейшей её передачи Эквайеру в установленном порядке.

Изъятые Карты подлежат хранению в специально оборудованных местах, обеспечивающих их сохранность и исключающих доступ посторонних лиц.

Срок хранения изъятых Карт определяется внутренними документами Участниками.

Доступ к изъятым Картам имеется только уполномоченных лиц Участника.

Изъятые Карты подлежат передаче Эмитенту по акту приёма-передачи либо надлежащему уничтожению, исключающему возможность восстановления и (или) дальнейшего использования, на основании соответствующего акта.

8. Мероприятия по противодействию мошенничеству, Операциям, связанным с незаконной игорной деятельностью и иным Операциям повышенного риска

8.1. Антифрод мероприятия

Оператор в целях обеспечения безопасности, стабильности и бесперебойности функционирования Системы, предотвращения мошенничества, несанкционированных Операций, а также минимизации рисков Участников, ПО и Держателей Карт вправе применять меры по ограничению, приостановлению и блокировке Операций и платежных инструментов, а также осуществлять изменение ПИН-кода Карты в порядке, предусмотренном настоящими Правилами.

Оператор вправе осуществлять мониторинг Операций, совершаемых в Системе, с использованием автоматизированных систем анализа рисков, антифрод систем, правил мониторинга, скоринговых моделей, а также иных инструментов выявления подозрительной активности.

Сбор информации о мошенничестве

Сбор информации о мошенничестве предназначен для централизованного выявления, анализа и предотвращения несанкционированных (фрод) Операций, совершённых с использованием ЭСП без согласия Клиента или с согласия, полученного под воздействием третьих лиц, а также для оперативного обмена информацией между Участниками, ПО и Оператором.

Подозрительная активность

Участники и ПО обязаны информировать Оператора о подозрительных и несанкционированных (фрод) Операциях с использованием ЭСП, о выявленных подозрительных Операциях, совершаемых в ТСП, которые могут быть связаны с компрометацией ЭСП, платежных инструментов, устройств самообслуживания, мошенничеством со стороны персонала ТСП, либо попытками совершения иных противоправных действий.

Оператор вправе без предварительного согласования с Участником, ПО либо Держателем Карты применять меры реагирования, предусмотренные настоящими Правилами, Нормативными документами Системы и законодательством Республики Узбекистан.

Порядок уведомления

Участники и ПО обязаны обеспечивать своевременное информирование Оператора о любых выявленных несанкционированных (фрод) Операциях и (или) подозрительной активности в ТСП.

Уведомление осуществляется в следующие сроки:

– Эмитент обязан направить Оператору сообщение о полученном от Клиента уведомлении о несанкционированной (фрод) Операции не позднее 5 (пяти) рабочих дней;

– Эквайер обязан направить Оператору сообщение о факте выявления подозрительного ЭСП (дроп-карта), участвующего в возможной мошеннической деятельности, а также о возможной компрометации ЭСП в сети устройств Эквайера незамедлительно по факту обнаружения данного типа Инцидента.

Сообщения направляются по согласованному с Оператором каналу коммуникации в свободной форме с указанием причины и деталей Операции с реквизитами ЭСП или платежного инструмента, необходимыми для идентификации их в Системе, либо в формате Оператора.

Формат предоставления данных сообщений доводится Оператором до Участников отдельным письмом через официальный канал коммуникации.

Запрос информации Оператором

Оператор в праве запрашивать у Участников или ПО сведения, необходимые для анализа мошеннической и другой подозрительной активности, включая информацию об Операциях, устройствах обслуживания, ТСП, случаях компрометации ЭСП и иных событиях.

Участник или ПО обязан ответить на запрос Оператора в течение 3 (трёх) рабочих дней.

Уведомления о рисках

Оператор в праве формировать и направлять Участникам и ПО уведомления, рекомендации и предупреждения о выявленных признаках мошеннической и другой подозрительной активности по Операциям с использованием ЭСП Участника или ПО, либо по Операциям в эквайринговой сети Участника.

Временные ограничения

В целях минимизации рисков несанкционированных (фрод) Операций Оператор вправе запрашивать подтверждение правомерности совершения Операции как у Участника или ПО, так и у Клиента Участника или ПО, а также принять меры реагирования, в случае невозможности получения подтверждения, и иные дополнительные меры ограничения, контроля либо специальные условия обработки отдельных категорий Операций.

Оператор вправе осуществлять блокировку Карты, Операций и/или денежных переводов не только в отношении Карты, по которой выявлены признаки мошеннической либо несанкционированной Операции, но и в отношении иных Карт, устройств либо участников цепочки переводов денежных средств, если по результатам анализа Операций имеются основания полагать, что такие Карты, устройства либо Операции связаны с противозаконными действиями, выводом либо транзитом денежных средств.

Оператор вправе применять меры, предусмотренные настоящим разделом:

– по собственной инициативе;
– на основании обращений Участников или ПО;
– на основании обращений Держателей Карт;
– на основании информации правоохранительных органов;
– на основании актов, предписаний, санкций, запросов либо иных документов государственных органов;
– на основании информации, полученной из антифрод систем, мониторинга либо иных источников.

Применение Оператором мер, предусмотренных настоящим разделом, не является нарушением обязательств Оператора перед Участниками, ПО либо Держателями Карт и не несет ответственности за убытки, ущерб, упущенную выгоду и т.п., причиненные применением предусмотренных настоящими Правилами ограничительных мер, если такие меры применены добросовестно, разумно и направлены на:

– обеспечение безопасности Системы;
– предотвращение ущерба;
– предотвращение мошенничества;
– исполнение требований законодательства Республики Узбекистан;
– исполнение требований уполномоченных государственных органов.

Оператор самостоятельно определяет:

– достаточность оснований для применения ограничительных мер;
– перечень применяемых мер;
– сроки действия ограничений;
– необходимость снятия ограничений.

Изменение ПИН-кода Карты

В целях повышения безопасности использования Карты, предотвращения ее несанкционированного использования, а также минимизации рисков, связанных с компрометацией

ПИН-кода или возникновением угрозы несанкционированного доступа к Карте, Держатель Карты вправе инициировать изменение ПИН-кода посредством ЭСП, обеспечивающего дистанционное взаимодействие с Держателем Карты.

Изменение ПИН-кода является Нефинансовой операцией и осуществляется Оператором на основании запроса Держателя Карты, сформированного и направленного посредством ЭСП. Предоставление ПО права обеспечивать изменение ПИН-кода Карты посредством ЭСП допускается исключительно по решению Оператора в отношении соответствующей ПО.

Участник, предоставляющий Держателю Карты ЭСП (либо ПО, предоставляющая такое ЭСП), посредством которого инициируется изменение ПИН-кода, обязан до направления соответствующего запроса Оператору обеспечить двухфакторную аутентификацию Держателя Карты, одним из обязательных факторов которой является биометрическая идентификация по изображению лица (Face ID).

Запрос на изменение ПИН-кода должен содержать волеизъявление Держателя Карты на изменение ПИН-кода соответствующей Карты, а также согласие Держателя Карты на обработку его персональных данных Оператором в объеме, необходимом для осуществления изменения ПИН-кода.

Направление запроса на изменение ПИН-кода Оператору допускается исключительно после успешного прохождения Держателем Карты предусмотренных настоящими Правилами процедур идентификации и аутентификации и подтверждения им согласия на обработку персональных данных.

Участник, предоставляющий соответствующее ЭСП (либо ПО, предоставляющая такое ЭСП), обеспечивает получение согласия Держателя Карты на обработку его персональных данных Оператором, формирование и передачу Оператору запроса на изменение ПИН-кода, а также фиксацию и хранение сведений, подтверждающих успешное прохождение Держателем Карты идентификации и аутентификации и предоставление указанного согласия.

Участник или ПО несет ответственность за надлежащее проведение идентификации и аутентификации Держателя Карты, получение необходимого согласия на обработку персональных данных и правомерность направления Оператору запроса на изменение ПИН-кода.

Оператор осуществляет изменение ПИН-кода на основании полученного запроса при условии его соответствия установленным Оператором требованиям и успешного прохождения предусмотренных Системой проверок.

Оператор вправе отказать в изменении ПИН-кода либо приостановить обработку запроса при непрохождении предусмотренных настоящими Правилами процедур идентификации и аутентификации, отсутствии согласия Держателя Карты на обработку персональных данных, выявлении признаков мошеннической или иной подозрительной активности, несоответствии запроса требованиям Системы либо технической невозможности его исполнения, а по запросам, направленным посредством ЭСП ПО, также при отсутствии решения Оператора о предоставлении соответствующей ПО права обеспечивать изменение ПИН-кода Карты.

Порядок формирования, передачи, обработки и исполнения запроса на изменение ПИН-кода, состав передаваемых сведений, требования к информационному взаимодействию, а также порядок фиксации результатов выполнения соответствующей Нефинансовой операции определяются настоящими Правилами и Нормативными документами Системы.

Сброс счетчика неправильных попыток ввода ПИН-кода является Нефинансовой операцией и осуществляется Оператором на основании соответствующего запроса Держателя Карты, сформированного и направленного посредством ЭСП.

До направления Оператору запроса на сброс счетчика неправильных попыток ввода ПИН-кода Участник, предоставляющий соответствующее ЭСП (либо ПО, предоставляющая такое ЭСП), обязан обеспечить двухфакторную аутентификацию Держателя Карты, одним из обязательных факторов которой является биометрическая идентификация по изображению лица (Face ID).

Порядок формирования, передачи и исполнения такого запроса определяется настоящими Правилами и Нормативными документами Системы.

Содействие расследованию

Участники и ПО обязаны оказывать Оператору содействие в расследовании случаев мошенничества, включая предоставление информации, журналов событий, сведений об Операциях и иных материалов, необходимых для анализа Инцидентов.

Канал коммуникации

В рамках системы противодействия мошенничеству обмен информацией между Участниками, ПО и Оператором осуществляется посредством электронной почты. Адрес электронной почты (cybersecurity@nmpc.uz) признаётся официальным каналом Оператора для передачи запросов, уведомлений, сообщений и иной информации, связанной с функционированием указанной системы.

Участники и ПО в пределах выполняемых ими функций обязаны незамедлительно исполнять требования и уведомления Оператора, связанные с:

- блокировкой Карт;
- ограничением Операций;
- предоставлением информации;
- проведением антифрод мероприятий;
- предотвращением мошеннических Операций.

8.2. Мероприятия по противодействию Операциям, связанным с незаконной игорной деятельностью и иным Операциям повышенного риска

В целях обеспечения устойчивого, безопасного и бесперебойного функционирования Системы, защиты прав и законных интересов Участников, ПО и Клиентов, предотвращения незаконного использования ЭСП, противодействия незаконной игорной деятельности, а также исполнения требований законодательства Республики Узбекистан Оператор обеспечивает функционирование системы мониторинга и противодействия Операциям, связанным с незаконной игорной деятельностью и иным Операциям повышенного риска (далее — Система мониторинга).

Система мониторинга представляет собой совокупность организационных, правовых и программно-технических средств, предназначенных для выявления, анализа, оценки, предотвращения, ограничения, приостановления и (или) блокирования Операций, содержащих признаки незаконной игорной деятельности, компрометации ЭСП, неправомерного использования платежной инфраструктуры, а также иных Операций, способных причинить ущерб Клиентам, Участникам, ПО либо Системе.

Полномочия Оператора

Оператор самостоятельно организует функционирование Системы мониторинга и вправе применять любые не запрещенные законодательством Республики Узбекистан организационные, технические и технологические меры, направленные на обеспечение безопасности Системы, защиты прав и законных интересов Участников, ПО и их Клиентов.

Для целей функционирования Системы мониторинга Оператор вправе:

- осуществлять непрерывный мониторинг всех Операций, совершаемых в Системе;
- применять автоматизированные системы, системы искусственного интеллекта, скоринговые модели, риск-движки, поведенческий анализ, системы мониторинга транзакционной активности и иные программно-технические средства;
- формировать собственные критерии, сценарии, правила, индикаторы и признаки подозрительных Операций;
- использовать сведения, полученные от Участников, ПО, государственных органов, правоохранительных органов, международных платежных систем, иных операторов платежных

систем, платежных организаций, банков, а также из иных законных источников;

– осуществлять централизованный учет случаев компрометации электронных средств платежа, выявленных дроп-карт, устройств самообслуживания, торгово-сервисных предприятий, реквизитов Операций и иных объектов мониторинга.

Мероприятия по противодействия незаконной игорной деятельности

В целях исполнения требований законодательства Республики Узбекистан Оператор обеспечивает функционирование подсистемы выявления и противодействия Операциям, связанным с незаконной игорной деятельностью.

Указанная подсистема предназначена для выявления, анализа, ограничения, приостановления либо блокирования Операций, имеющих признаки осуществления платежей:

– в пользу организаторов незаконных азартных игр;

– онлайн-казино;

– букмекерских контор;

– тотализаторов;

– иных основанных на риске игр;

– иных Операций, запрещенных либо ограниченных законодательством Республики Узбекистан, либо настоящими Правилами и нормативными документами Системы.

Полномочия Оператора по применению ограничительных мер

При наличии достаточных оснований Оператор вправе без предварительного согласования с Участником, ПО либо Держателем Карты:

– ограничить проведение Операции;

– приостановить проведение Операции;

– отклонить обработку Операции;

– временно ограничить использование ЭСП;

– временно приостановить использование Карты;

– заблокировать Карту;

– заблокировать ЭСП;

– установить дополнительные условия обработки отдельных категорий Операций;

– запросить дополнительное подтверждение Операции;

– принять иные необходимые меры.

Ограничительные меры могут применяться как в отношении конкретной Операции либо Карты, так и в отношении иных Карт, ЭСП, устройств самообслуживания, Терминалов, ТСП, Клиентов либо Участников цепочки движения денежных средств, если результаты анализа позволяют сделать вывод об их взаимосвязи с противоправной деятельностью.

Обмен информацией

Оператор вправе запрашивать любую информацию, необходимую для анализа подозрительной активности в рамках Системы.

Участники и ПО обязаны предоставить такую информацию в полном объеме в срок, указанный в соответствующем запросе Оператора.

Обмен информацией осуществляется посредством официальных каналов связи, определенных Оператором.

Электронный адрес (cybersecurity@nmpc.uz) признается официальным каналом взаимодействия по вопросам функционирования Системы мониторинга, если иной адрес не

предоставлен Оператором.

Освобождение Оператора от ответственности

Применение Оператором предусмотренных настоящими Правилами и Нормативными документами Системы ограничительных мер не является нарушением обязательств перед Участниками, ПО либо их Клиентами.

Оператор не несет ответственности за убытки, ущерб, упущенную выгоду, невозможность совершения Операций либо иные неблагоприятные последствия, возникшие вследствие добросовестного применения ограничительных мер, если такие меры были направлены на:

- обеспечение безопасности Системы;
- защиту денежных средств и данных Клиентов;
- предотвращение мошенничества;
- противодействие незаконной игорной деятельности;
- предотвращение легализации преступных доходов;
- исполнение требований законодательства Республики Узбекистан;
- исполнение требований Центрального банка Республики Узбекистан;
- исполнение требований уполномоченных государственных органов.

9. Система управления рисками в Системе

В Системе функционирует СУР, обеспечивающая выявление, оценку, мониторинг и контроль рисков, возникающих при функционировании Системы.

Оператор определяет уполномоченное подразделение (функцию) по координации СУР в Системе и закрепляет порядок работы СУР в Нормативных документах Системы.

Цели СУР:

- обеспечение бесперебойности функционирования Системы;
- снижение влияния неблагоприятных факторов на стабильность и безопасность Системы;
- своевременное выявление и предотвращение событий, способных повлиять на Систему;
- снижение последствий реализованных рисков.

СУР охватывает, как минимум, следующие категории рисков:

- Операционный риск;
- расчетный/клиринговый риск;
- риск мошенничества (антифрод);
- киберриски и риск информационной безопасности;
- правовой/комплаенс-риск;
- репутационный риск.

Порядок мониторинга рисков, обмена информацией, реагирования на Инциденты и применения контрольных мер устанавливается Нормативными документами Системы.

Требования настоящего раздела применяются с учетом положений раздела **10** (Защита информации) настоящих Правил.

10. Требования к обеспечению защиты информации

Требования настоящего раздела распространяются на Участников и ПО в пределах выполняемых ими функций, используемой информационной инфраструктуры и обрабатываемой информации.

В Системе обязанности по определению порядка обеспечения защиты информации при

осуществлении Операций с использованием Карт распределяются между Оператором, Участниками и ПО.

Участники и ПО принимают на себя обязательства по обеспечению защиты информации при осуществлении Операций в соответствии с требованиями Правил, Нормативных документов Системы, законодательства, а также обеспечивать выполнение требований международного стандарта PCI DSS.

В Правилах содержатся общие требования по обеспечению защиты информации.

Требования к обеспечению защиты информации применяются для обеспечения защиты следующей информации (далее - защищаемая информация):

– информации о совершенных Операциях, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников или ПО, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников или ПО;

– информации, содержащейся в оформленных, в рамках применяемой формы безналичных расчетов, распоряжениях Клиентов, Участников и ПО;

– информации, необходимой для удостоверения Клиентами права распоряжения денежными средствами, в том числе данных Держателей Карт;

– ключевой информации средств криптографической защиты информации, используемых при осуществлении Операций;

– информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участниками и (или) ПО и используемых для осуществления Операций;

– информации о конфигурации, определяющей параметры работы технических средств защиты информации;

– информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Республики Узбекистан, обрабатываемой при осуществлении Операций.

Каждый Участник или ПО самостоятельно определяет порядок обеспечения защиты информации в соответствии с законодательством, в том числе, с нормативно-правовыми актами Центрального банка в сфере информационной безопасности, Правилами и Нормативными документами Системы в рамках обязанностей (зон ответственности), установленных в Правилах.

Конкретные требования к защите информации при осуществлении Операций с использованием Карт, включая способы и методы обеспечения указанных требований, закрепляются Участниками и ПО в их внутренних документах.

Защита информации обеспечивается Участниками и (или) ПО путем реализации правовых, организационных и технических мер, направленных:

– на обеспечение защиты информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации;

– на соблюдение конфиденциальности информации.

Для проведения работ по защите информации Участниками или ПО могут привлекаться на договорной основе организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации и/или на осуществление деятельности по разработке и производству средств защиты конфиденциальной информации.

Участники и ПО обеспечивают выполнение третьими сторонами, привлекаемыми к

деятельности по оказанию услуг по переводу денежных средств, требований к обеспечению защиты информации с учетом перечня выполняемых ими Операций и используемых автоматизированных систем, программного обеспечения, средств вычислительной техники и телекоммуникационного оборудования.

10.1. Требования к Участникам и ПО по защите информации

Участники и (или) ПО обязаны обеспечивать защиту информации при осуществлении Операций с использованием Карт, при обмене электронными сообщениями, при хранении и обработке информации, связанной с их деятельностью в Системе, в соответствии с требованиями законодательства, Правил и Нормативных документов Системы.

Участники и (или) ПО должны обеспечить безопасность технологического процесса обработки, передачи и хранения защищаемой информации, согласованное применение технологических и организационных мер, технических и программных средств защиты информации на всех этапах подготовки, обработки, передачи и хранения защищаемой информации.

Требования к защите информации реализуются Участниками и ПО на всех стадиях жизненного цикла объектов информационной инфраструктуры.

Участники и (или) ПО обязаны обеспечить в отношении работников, участвующих в обработке, передаче и хранении защищаемой информации, связанной с их деятельностью в Системе:

– назначение прав и ролей, исходя из должностных обязанностей работников;

– контроль и регистрацию действий работников;

– выполнение процедур идентификации, аутентификации, авторизации при осуществлении доступа работников к защищаемой информации;

– реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с созданием (модернизацией), эксплуатацией и техническим обслуживанием объектов информационной инфраструктуры;

– реализацию запрета несанкционированного расширения прав доступа к защищаемой информации;

– назначение работникам минимально необходимых для выполнения ими функциональных обязанностей прав доступа к защищаемой информации;

– повышение осведомленности работников в области обеспечения защиты информации, порядка применения организационных мер и технических средств защиты информации;

– немедленный отзыв прав доступа работника при смене должностных обязанностей или увольнении.

Участники и (или) ПО обязаны обеспечить доступ своим работникам к объектам инфраструктуры, обрабатывающим защищаемую информацию, с применением:

– организационных мер и технических средств защиты, предназначенных для предотвращения несанкционированного доступа;

– систем контроля физического доступа;

– выполнение процедур идентификации, аутентификации, авторизации всех лиц при осуществлении доступа к защищаемой информации;

– регистрации действий всех лиц при осуществлении доступа к защищаемой информации.

Участники и (или) ПО при осуществлении Операций обеспечивают применение:

– средств криптографической защиты информации;

– средств защиты информации от несанкционированного доступа;

– средств антивирусной защиты;

– средств межсетевого экранирования;

– систем обнаружения вторжений;

– средства контроля (анализа) защищенности.

Для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - вредоносный код) Участники и (или) ПО обеспечивают:

– использование антивирусного программного обеспечения и его функционирование в автоматическом режиме на средствах вычислительной техники, включая Банкоматы и Терминалы, при наличии технической возможности;

– формирование для Клиентов рекомендаций по защите информации от воздействия вредоносного кода;

– использование антивирусного программного обеспечения различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления Операций, а также на межсетевых экранах, задействованных в осуществлении Операций, при наличии технической возможности;

– регулярное обновление версий антивирусного программного обеспечения и антивирусных баз данных, содержащих описание вредоносных кодов и способы их обезвреживания;

– выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая Банкоматы и Терминалы;

– выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая Банкоматы и Терминалы, выполняемой после установки или изменения программного обеспечения.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участники и (или) ПО:

– обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и на устранение последствий воздействия вредоносного кода;

– при необходимости приостанавливают осуществление Операций на период устранения последствий заражения вредоносным кодом;

– Участники и (или) ПО обеспечивают информирование Оператора и других Участников и ПО об Инциденте, связанном с обнаружением вредоносного кода или факта воздействия вредоносного кода.

При использовании сети Интернет для осуществления Операций Участники и (или) ПО обеспечивают:

– применение организационных мер защиты информации и/или использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к содержанию защищаемой информации, передаваемой по сети Интернет;

– применение организационных мер защиты информации и/или использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети Интернет;

– применение организационных мер защиты информации и/или использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения;

– минимизацию негативных последствий, связанных с несвоевременностью осуществления

Операций, сбоям или отказам в работе объекта информационной инфраструктуры;

– фильтрацию сетевых пакетов при обмене информацией между информационно коммуникационными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет с целью защиты от негативного внешнего воздействия из сети Интернет.

Участники и (или) ПО обеспечивают осуществление мероприятий, имеющих целью определение угроз безопасности информации и анализ уязвимости информационных систем.

10.2. Выявление Инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении Операций в Системе

Участники и (или) ПО в зоне своей ответственности обеспечивают выявление Инцидентов, реагирование на выявленные Инциденты, устранение причин возникновения Инцидентов, принятие всех необходимых мер по снижению негативных последствий Инцидент и мер по недопущению повторного возникновения Инцидентов.

Участники и (или) ПО ежемесячно информируют Оператора о выявленных Инцидентах, в порядке и сроки, устанавливаемые Оператором.

В случаях выявления Инцидентов, влияющих на безопасность функционирования Системы, Участники и (или) ПО незамедлительно информируют о них Оператора в порядке, предусмотренном Нормативными документами Системы.

Оператор после получения указанного выше уведомления обеспечивает осуществление всех возможных действий, направленных на устранение Инцидента, и уведомляет соответствующего Участника и (или) ПО о принятых мерах и их результатах.

Оператор обеспечивает учет и доступность для Участников и (или) ПО на ресурсах Системы:

– информации о выявленных Инцидентах, носящих системный характер;

– информации о практиках и методиках анализа и реагирования на Инциденты.

10.3. Обеспечение совершенствования защиты информации при осуществлении Операций в Системе

Участники и (или) ПО обеспечивают пересмотр порядка обеспечения защиты информации в случаях изменения требований к защите информации, определенных настоящими Правилами и законодательством Республики Узбекистан.

Участники и (или) ПО обеспечивают совершенствование защиты информации при осуществлении Операций в случаях:

– изменения требований к защите информации, определенных настоящими Правилами;

– изменений в законодательстве Республики Узбекистан;

– изменения порядка обеспечения защиты информации при осуществлении Операций;

– выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении Операций;

– выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении Операций.

11. Ответственность

За неисполнение или ненадлежащее исполнение Участниками и (или) ПО своих обязательств Участники и (или) ПО несут ответственность в соответствии с Правилами, Нормативными документами Системы, договорами и законодательством Республики Узбекистан.

Ответственность Участников и ПО Системы за соблюдение Правил наступает с момента присоединения к Правилам.

Ответственность Субъектов Системы за нарушения своих обязательств, распределяется следующим образом:

– Расчетный центр:
  - несет ответственность перед Участниками за неоказание/ненадлежащее оказание расчетных услуг в соответствии с договором.
– Оператор:
  - несет ответственность перед Участниками за неисполнение/ненадлежащее исполнение своих обязательств в соответствии с договорами Процессинга;
  - обязан возместить Участникам причиненные убытки, возникшие в результате неисполнения своих обязательств, в документально подтвержденном размере.
– Участники и ПО:
  - несут ответственность перед Субъектами Системы за свои действия/бездействия в рамках Системы, а также за действия/бездействия третьих лиц, привлеченных соответствующим Участником или соответствующей ПО для осуществления деятельности в Системе (включая мошеннические и другие противоправные действия), в том числе за нарушение Правил и Нормативных документов Системы, возникшие по вине соответствующего Участника или соответствующей ПО;
  - обязаны возместить иным Субъектам Системы в полном объеме документально подтвержденный ущерб, нанесенный в результате этих действий/бездействий;
  - обязаны возместить иным Субъектам Системы документально подтвержденные убытки, причиненные им действиями/бездействиями соответствующего Участника или соответствующей ПО, а также действиями/бездействиями третьих лиц, привлеченных Участниками или ПО для осуществления деятельности в рамках Системы.

Участники и ПО несут ответственность за неисполнение/ненадлежащее исполнение условий размещения и использования товарного знака, знака обслуживания и Логотипа Системы, установленных Правилами, в том числе за искажение товарного знака и знака обслуживания Системы.

В случае применения к Участнику или ПО мер воздействия Оператор направляет ему соответствующее уведомление посредством официального канала коммуникации. Уведомление должно содержать, в том числе, следующую информацию:

– вид примененной меры воздействия;

– основания и обстоятельства, послужившие причиной применения меры воздействия, с указанием нарушенных требований Правил, Нормативных документов Системы либо законодательства Республики Узбекистан (при наличии);

– размер штрафа, подлежащего уплате, если применение меры воздействия предусматривает наложение финансовых санкций;

– срок и порядок устранения выявленных нарушений (при необходимости);

– информацию о праве Участника или ПО представить письменные объяснения, возражения, дополнительные документы либо обжаловать применение меры воздействия и (или) размер наложенных финансовых санкций в порядке, предусмотренном настоящими Правилами и/или Нормативными документами Системы.

При необходимости Оператор вправе потребовать от Участника и (или) ПО в установленный Оператором срок представить план мероприятий по устранению выявленных нарушений, а также документы и сведения, подтверждающие их устранение. Перечень сведений, содержащихся в уведомлении, не является исчерпывающим, и Оператор вправе включить в него иную информацию, необходимую для исполнения Участником и (или) ПО требований Оператора и настоящих Правил.

Уведомление может быть направлено любым доступным Оператору способом, позволяющим

подтвердить факт получения Участником и (или) ПО данного уведомления.

В случае несогласия с выявленным нарушением Участник и (или) ПО имеет право в течение 10 (десяти) календарных дней с момента получения уведомления Оператора о нарушении направить Оператору письменное возражение, содержащее обоснование позиции Участника и (или) ПО.

Направление Участником и (или) ПО возражения не освобождает от уплаты штрафа.

Оператор рассматривает возражение Участника и (или) ПО в срок не менее 15 (пятнадцати) рабочих дней с даты его получения.

В случае принятия Оператором положительного решения по итогам рассмотрения возражения Участника и (или) ПО взысканная сумма штрафа возвращается Участнику и (или) ПО в течение 10 (десяти) рабочих дней. Участники и (или) ПО освобождаются от ответственности за частичное или полное неисполнение/ненадлежащее исполнение своих обязательств, определенных Правилами, Нормативными документами Системы, если это неисполнение/ненадлежащее исполнение явилось следствием обстоятельств непреодолимой силы («форс-мажор).

К обстоятельствам непреодолимой силы относятся события, на которые Участники и (или) ПО не могут оказать влияния и за возникновение которых они не несут ответственности, такие как войны и вооруженные конфликты, запретительные акты и действия государственных органов.

При наступлении обстоятельств непреодолимой силы, препятствующих исполнению обязательств Участниками и (или) ПО, срок выполнения таких обязательств переносится соразмерно времени действия таких обстоятельств, а также времени, требуемого для устранения их последствий.

Участники и (или) ПО обязаны незамедлительно любыми доступными способами уведомить Оператора о наступлении обстоятельств непреодолимой силы и немедленно направить уведомление в письменной форме по любому из доступных каналов связи (почта, факс, электронная почта и др.). Уведомление должно содержать данные о характере обстоятельств и, по возможности, информацию, позволяющую дать оценку их влияния на возможность исполнения Участниками принятых на себя обязательств в рамках Системы.

Факт возникновения обстоятельств непреодолимой силы и срок их действия должен быть подтвержден соответствующим государственным органом, в ведении которого относится констатация (удостоверение) подобных обстоятельств.

Если Участник и (или) ПО не направит или несвоевременно направит уведомление, то он обязан возместить другим Участникам и (или) ПО, понесенные ими убытки и не вправе ссылаться на обстоятельства непреодолимой силы.

По прекращении действия указанных обстоятельств Участник и (или) ПО, который не в состоянии был выполнить свои обязательства в силу возникновения обстоятельств непреодолимой силы, обязан в срок до 3 (трех) рабочих дней после прекращения их действия известить об этом Оператора в письменной форме.

Оператор не несёт ответственности за какие-либо убытки Участников и (или) ПО, включая прямые, косвенные, последующие и производные убытки, упущенную выгоду, потери дохода, утрату данных, вред деловой репутации, регуляторные последствия, штрафы, санкции, пени, неустойки, судебные издержки, а также любые иные имущественные и неимущественные потери, даже в случае, если Участник и (или) ПО был уведомлён о возможности наступления таких последствий.

Участник несет полную ответственность за законность, достоверность, полноту, корректность, актуальность и обоснованность сведений, содержащихся в направляемых Оператору клиринговых файлах, а также за соблюдение требований законодательства Республики Узбекистан, настоящих Правил и Нормативных документов Системы при их формировании и направлении.

Обработка Оператором клирингового файла не означает подтверждение законности, правильности, достоверности, обоснованности либо действительности содержащихся в нем Операций и не свидетельствует о принятии Оператором ответственности за содержание такого

файла.

Все разногласия, споры, претензии и требования, связанные с содержанием клиринговых файлов, отраженными в них Операциями, суммами взаиморасчетов, принадлежностью Операций, основаниями их совершения, а также иными сведениями, содержащимися в клиринговых файлах, подлежат урегулированию непосредственно между соответствующими Участниками без участия Оператора, если иное не предусмотрено законодательством Республики Узбекистан либо настоящими Правилами.

Оператор не является стороной правоотношений между Участниками и (или) ПО, возникающих в связи с совершением платежных Операций, не рассматривает споры по существу таких правоотношений и не принимает решения о наличии либо отсутствии обязательств одного Участника и (или) ПО перед другим.

При возникновении разногласий между Участниками и (или) ПО Оператор в пределах своих полномочий оказывает содействие их урегулированию путем предоставления имеющейся у него информации, журналов обработки Операций, логов, сведений о прохождении сообщений, клиринговых файлов и иной информации, которой располагает Оператор, при условии соблюдения требований законодательства Республики Узбекистан, настоящих Правил и режима конфиденциальности. Предоставление такой информации не означает признание Оператором обоснованности требований какой-либо из сторон спора и не влечет возникновения у Оператора ответственности за разрешение такого спора.

Оператор не несет ответственности за последствия обработки клиринговых файлов, сформированных и направленных Участниками, если такие последствия вызваны недостоверностью, неполнотой, ошибочностью, несвоевременностью либо неправомерностью сведений, содержащихся в соответствующих клиринговых файлах, за исключением случаев, когда такие последствия возникли вследствие умышленных действий либо грубой неосторожности самого Оператора.

Штрафные санкции

Штрафные санкции применяются Оператором в случае нарушения Участником и (или) ПО требований настоящих Правил, Нормативных документов Системы, обязательных для исполнения требований (предписаний) Оператора, а также иных обязательств, предусмотренных законодательством Республики Узбекистан.

Штрафные санкции применяются к Участнику или ПО исключительно за нарушения требований, относящихся к осуществляемой им деятельности, выполняемым функциям и предоставленным ему функциональным возможностям в рамках Системы.

Применение к ПО штрафных санкций за нарушение требований, относящихся исключительно к деятельности Участника, Эмитента или Эквайера, включая требования, связанные с Эмиссией Карт, Эквайрингом, использованием БИНов, ведением Счета Участника, клирингом и расчетами между Участниками, не допускается, если соответствующие функции прямо не возложены на ПО законодательством Республики Узбекистан, настоящими Правилами или соглашением о взаимодействии с Оператором.

Целью применения штрафных санкций является обеспечение надлежащего исполнения требований Системы, предупреждение и пресечение нарушений, обеспечение стабильного, безопасного и бесперебойного функционирования Системы, защита прав и законных интересов Участников, ПО, Клиентов и Оператора.

Основанием для применения штрафных санкций является мотивированное решение Оператора, принятое по результатам рассмотрения материалов, подтверждающих факт нарушения.

При принятии решения о применении штрафных санкций Оператор вправе учитывать характер, степень, продолжительность и последствия нарушения, наличие повторности нарушений, размер причиненного либо потенциального ущерба, наличие обстоятельств, смягчающих или отягчающих ответственность, действия Участника или ПО по предотвращению и устранению

последствий нарушения, степень его содействия Оператору а также иные обстоятельства, имеющие значение для объективного рассмотрения вопроса.

Оператор самостоятельно определяет необходимость применения штрафных санкций, их размер, а также иные меры воздействия в пределах, предусмотренных настоящими Правилами и Нормативными документами Системы, исходя из принципов разумности, добросовестности, соразмерности допущенному нарушению и необходимости обеспечения безопасности и стабильности функционирования Системы.

Для целей настоящего раздела повторным признается аналогичное нарушение, совершенное Участником или ПО после применения к нему меры воздействия за предыдущее аналогичное нарушение в течение двенадцати месяцев с даты принятия Оператором соответствующего решения, если иной период не установлен настоящими Правилами или Нормативными документами Системы.

Решение Оператора о применении штрафных санкций должно содержать:

– наименование Оператора;

– номер, дату и место принятия решения;

– сведения об Участнике или ПО, допустивших нарушение;

– описание выявленного нарушения;

– обстоятельства и основания применения штрафной санкции;

– ссылку на нарушенные положения настоящих Правил, Нормативных документов Системы, обязательного требования (предписания) Оператора или соответствующего договора, либо законодательства Республики Узбекистан (при наличии);

– сведения о материалах, подтверждающие факт нарушения;

– вид и размер применяемой штрафной санкции;

– срок устранения нарушения (при необходимости);

– срок уплаты штрафа;

– информацию о праве Участника или ПО представить письменные объяснения, возражения либо обжаловать принятое решение в порядке, установленном настоящими Правилами.

Решение Оператора направляется Участнику или ПО посредством официального канала коммуникации и считается полученным с момента его направления, если иной момент получения не подтвержден документально.

Штраф подлежит уплате в течение 10 (десяти) рабочих дней со дня получения решения Оператора, если иной срок не установлен таким решением Оператора.

Уплата штрафа не освобождает Участника или ПО от обязанности устранить допущенное нарушение, исполнить обязательные требования Оператора, исполнить возникшие финансовые и иные обязательства, а также возместить причиненные убытки в случаях и порядке, предусмотренных законодательством Республики Узбекистан, настоящими Правилами, Нормативными документами Системы либо соответствующими договорами.

Применение штрафных санкций не ограничивает право Оператора одновременно либо последовательно применять к Участнику или ПО иные меры воздействия, предусмотренные настоящими Правилами, Нормативными документами Системы, включая предупреждение, выдачу обязательного для исполнения предписания, ограничение или приостановление отдельных Операций, ограничение доступа к отдельным сервисам Системы, временное приостановление обслуживания либо прекращение участия Участника в Системе либо прекращение взаимодействия с ПО в случаях, предусмотренных настоящими Правилами и Нормативными документами Системы.

Размеры штрафных санкций

Общие нарушения Участников и Платежных организаций

За неисполнение или несвоевременное исполнение обязательного требования (предписания) Оператора, в том числе непредоставление в установленный срок запрошенных документов, информации, сведений или пояснений, — штраф в размере до 50 БРВ.

За предоставление Оператору заведомо недостоверной или искаженной информации, повлекшее либо способное повлечь нарушение функционирования Системы, некорректную обработку Операций или возникновение финансовых потерь, — штраф в размере до 100 БРВ.

За неисполнение обязанности по уведомлению Оператора об Инцидентах, нарушениях безопасности и иных событиях, о которых Участник или ПО обязан уведомить Оператора в соответствии с настоящими Правилами или Нормативными документами Системы, — штраф в размере до 100 БРВ.

За нарушение обязательных требований Оператора, направленных на обеспечение безопасности, стабильности и бесперебойного функционирования Системы, если для соответствующего нарушения настоящими Правилами или Нормативными документами Системы не предусмотрена специальная штрафная санкция, — штраф в размере до 100 БРВ.

Нарушения Участников

За неправильное присвоение или несвоевременную актуализацию MCC-кода ТСП, предоставление недостоверных сведений о категории деятельности ТСП, в том числе в целях снижения размера комиссионного вознаграждения либо обхода установленных ограничений:

- за первое выявленное нарушение — предупреждение и (или) штраф в размере до 50 БРВ;
- за повторное нарушение — штраф до 100 БРВ.

За нарушение установленных требований к использованию предоставленных Участнику БИНов, в том числе передачу права их использования третьим лицам, использование БИНа не по назначению либо иное нарушение установленного порядка использования БИНов, повлекшее или способное повлечь некорректную маршрутизацию или обработку Операций, — штраф в размере от 100 до 500 БРВ.

За нарушение требований Авторизации, маршрутизации, обработки или подтверждения Операций, а также проведение Операций без предусмотренной настоящими Правилами или Нормативными документами Системы Авторизации — штраф в размере от 100 до 500 БРВ.

За некорректную регистрацию Терминалов, Банкоматов или иных устройств в Системе либо несвоевременное обновление сведений о таких устройствах, если это повлекло или могло повлечь некорректную обработку Операций, — штраф в размере от 50 до 200 БРВ.

За использование Терминалов, включая E-POS, M-POS, иных устройств или программных решений не по их функциональному назначению, а также изменение параметров Операций, типов Операций (Transaction Type), способов обработки платежей или иных реквизитов Операций в целях обхода требований или ограничений Системы — штраф в размере 20 (двадцати) процентов от общей суммы Операций, совершенных с соответствующим нарушением, но не менее 200 БРВ.

За нарушение требований настоящих Правил и Нормативных документов Системы при Эмиссии Карт, включая использование БИНа, не предоставленного соответствующему Участнику, либо выпуск Карт с нарушением установленных требований Системы, — штраф в размере от 100 до 500 БРВ.

За нарушение Эквайером требований по проверке ТСП до принятия его на эквайринговое обслуживание, присвоению и актуализации MCC-кода, обеспечению безопасного функционирования Сети устройств либо иных обязательных требований, установленных для Эквайера настоящими Правилами, — штраф в размере от 100 до 500 БРВ.

Нарушения Платежных организаций

За использование ПО инфраструктуры, сервисов или функциональных возможностей Системы за пределами, предоставленных ей Оператором функциональных возможностей либо с нарушением

условий взаимодействия, установленных настоящими Правилами, Нормативными документами Системы или соглашением о взаимодействии с Оператором, — штраф в размере до 200 БРВ.

За нарушение ПО установленных требований к идентификации и аутентификации Клиентов и (или) Держателей Карт при использовании ЭСП, в том числе при инициировании Операций и Нефинансовых операций, — штраф в размере до 200 БРВ.

За нарушение ПО требований к формированию, подтверждению, передаче или хранению запросов и иных сведений, передаваемых Оператору посредством ЭСП, направление таких запросов без прохождения предусмотренных процедур идентификации и аутентификации Держателя Карты, а также при отсутствии необходимого согласия на обработку и передачу персональных данных — штраф в размере до 200 БРВ.

За нарушение ПО требований настоящих Правил и Нормативных документов Системы к обеспечению безопасности ЭСП и информационно-технологического взаимодействия с Системой, если такое нарушение повлекло или могло повлечь несанкционированный доступ, неправомерное совершение Операций, компрометацию данных либо нарушение функционирования Системы, — штраф в размере до 500 БРВ.

Иные нарушения

За нарушение требований настоящих Правил, Нормативных документов Системы или обязательных требований (предписаний) Оператора, для которого настоящими Правилами или Нормативными документами Системы не установлен отдельный размер штрафной санкции, Оператор вправе применить штраф в размере до 200 БРВ с учетом характера, степени и последствий допущенного нарушения.

Если одно действие или бездействие содержит признаки нескольких нарушений, штрафная санкция применяется за каждое самостоятельное нарушение, если соответствующие нарушения имеют различные объекты и последствия. При этом совокупный размер применяемых штрафных санкций должен быть соразмерен характеру и последствиям допущенных нарушений.

Применение штрафной санкции не препятствует возмещению Участником или ПО документально подтвержденных убытков, причиненных Оператору или иным лицам, если обязанность по их возмещению предусмотрена законодательством Республики Узбекистан, настоящими Правилами или соответствующим договором.

Изменение видов нарушений и размеров штрафных санкций осуществляется путем внесения изменений и дополнений в настоящие Правила и (или) Нормативные документы Системы в порядке, установленном настоящими Правилами.

12. Разрешение споров (диспутов)

Оператор, Участники и ПО обязуются урегулировать возникающие между ними диспутных случаев (споры) добросовестно и своевременно.

Взаимодействие между Участником и (или) ПО и Оператором в рамках урегулирования диспутных случаев осуществляется через электронную почту (dispute@nmpc.uz) и (или) через специализированную платформу (личный кабинет), предоставленный Оператором каждому Участнику или ПО, и признаётся официальным каналом для передачи запросов, уведомлений, сообщений, документов и иной информации, связанной с урегулированием диспутов.

ПО участвует в рассмотрении и урегулировании Диспутов исключительно в части Операций, услуг, ЭСП и иных действий, относящихся к деятельности такой ПО в рамках Системы.

Участники и ПО обязуются назначать специальных работников для управления процедурой урегулирования диспутных Операций и стремиться оказывать содействие другим Участникам или ПО в урегулировании диспутных Операций между следующими сторонами:

- Держателем Карты и ТСП другого Участника;
- ТСП и Держателем Карты другого Участника;

– при урегулировании иных диспутных Операций между Участниками, ПО, Оператором и иными лицами, связанными с соответствующей Операцией.

Оператор вправе осуществлять безакцептное (в рамках клирингового цикла) списание, удержание и (или) взаимозачёт денежных средств Участника в целях исполнения распределения финансовой ответственности между Участниками в рамках диспутного процесса, включая случаи, когда Участник принимает диспутную Операцию и (или) финансовую ответственность по ней, либо не предоставляет запрошенные в установленные сроки документы, сведения или пояснения, либо иным образом уклоняется от участия в диспутном процессе.

Порядок исполнения ПО финансовых обязательств, возникающих в связи с диспутным процессом, определяется соглашением о взаимодействии, заключенным между Оператором и соответствующей ПО, и Нормативными документами Системы.

При урегулировании споров любые документы или файлы/чеки, которые могут подтвердить/доказать подлинность Операции, могут считаться приемлемой заменой стандартных квитанций/документов, предусмотренных Правилами.

Порядок рассмотрения, сопровождения и урегулирования диспутных Операций определяется настоящими Правилами и Нормативными документами Оператора и доводится до сведения Участников и ПО путём размещения на Информационном ресурсе Системы.

13. Конфиденциальность

Под конфиденциальной информацией Участника и (или) ПО понимается информация ограниченного доступа, в том числе составляющая коммерческую тайну Участников и (или) ПО, а также любая иная принадлежащая Участнику и (или) ПО информация независимо от формы ее предоставления, передаваемая раскрывающей стороной принимающей стороне.

Требования настоящего раздела распространяются на Оператора, Участников, ПО и Расчетный центр, каждый из которых в зависимости от обстоятельств может выступать раскрывающей или принимающей стороной.

Конфиденциальной информацией Системы признается любая информация, связанная с функционированием Системы, доступ к которой ограничен в соответствии с законодательством Республики Узбекистан, настоящими Правилами, договорами с Участниками и (или) соглашениями о взаимодействии с ПО, заключенными Оператором, а также внутренними документами Оператора.

К конфиденциальной информации Системы относятся, в том числе:

– сведения о программном обеспечении, архитектуре, технических решениях, информационной инфраструктуре и средствах защиты информации Системы;

– сведения о технологиях обработки Операций, маршрутизации, авторизации, клиринга, расчетов и иных технологических процессах Системы;

– криптографические ключи, средства криптографической защиты информации, параметры безопасности, а также иные сведения, связанные с обеспечением информационной безопасности Системы;

– сведения, полученные Оператором, Участниками и (или) ПО при осуществлении деятельности в рамках Системы, если такие сведения отнесены к информации ограниченного доступа в соответствии с законодательством Республики Узбекистан, настоящими Правилами или договорами;

– иная информация, определенная Оператором как конфиденциальная, при условии, что такой режим не противоречит законодательству Республики Узбекистан.

Не относится к конфиденциальной информации Системы информация, которая:

– является общедоступной либо стала общедоступной не вследствие нарушения настоящих Правил;

– подлежит раскрытию в соответствии с законодательством Республики Узбекистан;

– правомерно получена от третьих лиц без нарушения обязательств по соблюдению конфиденциальности;

– раскрывается на основании требований суда либо иных государственных органов в пределах их компетенции в соответствии с законодательством Республики Узбекистан.

Для обеспечения конфиденциальности, целостности и неотказуемости информации в рамках деятельности в Системе Участники и (или) ПО обязаны использовать систему электронного документооборота и защищенные каналы связи, позволяющие при информационном обмене между Участниками передавать документы в защищенном (зашифрованном) виде, подписанные с использованием электронной подписи стороны, сформировавшей документ.

Передача конфиденциальной информации по открытым каналам связи запрещена. Принимающая сторона не вправе без письменного согласия (разрешения) Раскрывающей стороны разглашать или иным образом раскрывать конфиденциальную информацию третьим лицам, за исключением случаев, предусмотренных Правилами, законодательством Республики Узбекистан.

Участники и (или) ПО принимают на себя обязательства сохранять конфиденциальность информации, используемой и получаемой при осуществлении деятельности в Системе, и вправе, без предварительного письменного согласия Раскрывающей стороны, по своему усмотрению и с учетом разумной необходимости передавать ее своим работникам, которым такая информация необходима для работы в Системе и которые допущены к работе с конфиденциальной информацией.

Принимающая сторона несет ответственность за действия (бездействие) своих работников и иных лиц, получивших доступ к конфиденциальной информации.

Принимающая сторона несет ответственность за разглашение конфиденциальной информации, а также за несанкционированное использование конфиденциальной информации, произошедшие по вине принимающей стороны.

Принимающая сторона обязана возместить раскрывающей стороне убытки, возникшие в результате разглашения конфиденциальной информации или ее несанкционированного использования, произошедшие по вине Принимающей стороны.

В случае прекращение участия Участника в Системе либо прекращение взаимодействия ПО с Оператором, а также в любое время по требованию Раскрывающей стороны Принимающая сторона обязана будет возвратить Раскрывающей стороне по акту всю ранее переданную ей конфиденциальную информацию, а также все копии, любые отчеты, анализы, справки, выписки, репродукции и иные материалы, содержащие конфиденциальную информацию (как в письменной, так и в электронной форме), находящуюся в ее владении и во владении лиц, которым конфиденциальная информация была раскрыта в соответствии с условиями Правил, в течение 5 (пяти) рабочих дней со дня получения уведомления Раскрывающей стороны о возврате ей конфиденциальной информации, а в случае невозможности передачи – уничтожить ее (их) и предоставить Раскрывающей стороне акт об уничтожении в течение 5 (пяти) рабочих дней со дня получения уведомления Раскрывающей стороны об уничтожении конфиденциальной информации. В случае невозможности возврата и (или) уничтожения конфиденциальной информации в сроки, установленные выше, данный срок может быть изменен по соглашению сторон.

В случае прекращение участия Участника в Системе либо прекращение взаимодействия ПО с Оператором по любому основанию обязательства по неразглашению конфиденциальной информации сохраняются в течение 5 (пяти) лет со дня прекращения участия Участника в Системе либо прекращения взаимодействия ПО с Оператором.