

Протокол внесения изменений в Правила Платежной системы «ХЕЛЛО»

Дата вступления в силу	Номер редакции Правил	Описание
28 июля 2022 года	Редакция № 2	<p>1. Пункт 2.5.1 Правил изложен в новой редакции. Старая редакция: «Расчетным центром платежной системы может выступать кредитная организация, созданная в соответствии с законодательством РФ, в том числе небанковская кредитная организация, находящаяся на территории Российской Федерации, осуществляющая не менее двух лет деятельность по переводу денежных средств по открытым в этой кредитной организации банковским счетам.» Новая редакция: «Расчетным центром платежной системы может выступать кредитная организация, созданная в соответствии с законодательством РФ, в том числе небанковская кредитная организация, находящаяся на территории Российской Федерации, осуществляющая не менее одного года деятельность по переводу денежных средств по открытым в этой кредитной организации банковским счетам.»</p> <p>2. Пункт 5.6.1. Правил изложен в новой редакции. Старая редакция: «Партнеры Платежной системы «ХЕЛЛО» - юридические лица, в т.ч. имеющие лицензию (разрешение) на осуществление переводов денежных средств, почтовых переводов в соответствии с законодательством страны своего местонахождения, не присоединившиеся к Правилам Системы в целом, осуществляющие перевод в качестве клиентов Участников, в т.ч. Оператора Системы, в соответствии с Правилами Системы и соответствующими соглашениями, заключенными с Участниками, в т.ч. с Оператором Системы.» Новая редакция: «Партнеры Платежной системы «ХЕЛЛО» - юридические лица, в т.ч. имеющие лицензию (разрешение) на осуществление переводов денежных средств, почтовых переводов в соответствии с законодательством страны своего местонахождения, не присоединившиеся к Правилам Системы в целом, осуществляющие перевод в качестве клиентов Участников, в соответствии с Правилами Системы и соответствующими соглашениями, заключенными с Участниками.»</p> <p>3. Пункт 7.2. дополнен подпунктом 7.2.15.:</p>

		<p>«В рамках Положения № 719-П Оператор определяет требования к обеспечению защиты информации, управляет риском информационной безопасности в Системе, выявляя недостатки следующих процессов в своей инфраструктуре, а также в инфраструктурах Субъектов ПС:</p> <ul style="list-style-type: none">• технологических мер защиты информации;• прикладного программного обеспечения. <p>Участники ПС реализуют процессы выявления, идентификации и анализа рисков информационной безопасности в отношении своих объектов информационной инфраструктуры, включая процессы реагирования на инциденты связанные с защитой информации и восстановления их штатного функционирования.</p> <p>Оператор также определяет следующие мероприятия по управлению риском информационной безопасности в отношении Субъектов Системы:</p> <ul style="list-style-type: none">• определение порядка обеспечения защиты информации, системы управления риском ИБ Оператора Системы в целом, включая выполняемые им функции оператора УПИ, которые фиксируются во внутренних документах Оператора Системы, не являющихся публичными;• управление риском ИБ в Системе;• определение требований к защите информации;• определение состава показателей уровня риска ИБ в Системе;• реализация Участниками и операторами УПИ механизмов, направленных на• соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения Участниками и операторами УПИ;• обеспечение реализации Участниками и операторами УПИ процессов выявления и идентификации риска ИБ в Системе в отношении объектов информационной инфраструктуры Участников и операторов УПИ;• выявление и анализ Участниками и операторами УПИ риска ИБ;• установление порядка, формы и сроков информирования Оператора Системы, Участников Системы и операторов УПИ о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации;• определение порядка взаимодействия Субъектов Системы в случае выявления в Системе вышеуказанных инцидентов;• обеспечение реализации Участниками и операторами УПИ процессов реагирования на инциденты защиты информации и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации;• установление требований к реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента;• ведение Оператором базы событий инцидентов, приведших к реализации риска ИБ;• в рамках проведения анализа рисков осуществление Оператором оценки соблюдения в Системе установленных требований к защите информации;
--	--	--

		<ul style="list-style-type: none"> • реализация Оператором процессов применения в отношении Участников и операторов УПИ ограничений по параметрам операций в случае выявления факта превышения значений показателей уровня риска, в том числе условий снятия таких ограничений. <p>4. Пункт 8.3. дополнен следующими подпунктами: «Выявление и идентификацию, анализ рисков нарушения своего надлежащего функционирования в рамках Системы, в т.ч. риска ИБ, в отношении объектов информационной инфраструктуры участников платежной системы и операторов УПИ, оценку эффективности методик анализа и минимизации выявленных рисков, а также выявление новых рисков в рамках внутренних систем управления рисками в своей деятельности в части выполнения функций Участника</p> <p>Выявление и анализ рисков нарушения надлежащего функционирования в рамках Системы, в т.ч. риска ИБ, в отношении объектов информационной инфраструктуры участников платежной системы и операторов УПИ, оценку эффективности методик анализа и минимизации выявленных рисков, а также выявление новых рисков в рамках внутренних систем управления рисками своей деятельности в части выполнения функций оператора УПИ.»</p> <p>5. Пункт 14.6 дополнен следующим подпунктом: «Выявление и анализ риска информационной безопасности в Платежной Системе. Включает в себя определение источников риска и событий, реализация которых может привести к возникновению инцидента (риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации; анализ возможностей на проникновение, при тестировании каждой области оценивается процесс реагирования на инциденты информационной безопасности и возможности по восстановлению работоспособности, в случае возможной компрометации безопасности ИТ систем; использование специализированного программного обеспечения для выявления уязвимостей программного и аппаратного обеспечения; непрерывный мониторинг событий ИБ;»</p> <p>6. Пункт 14.8. дополнен показателями уровня риска информационной безопасности для Операционного и Платежно-клирингового центров.</p> <p>7. Пункт 14.13.2. дополнен требованием Оператора Системы к Участникам и привлеченному Расчетному центру предоставлением информации об используемых СКЗИ.</p> <p>8. Пункт 14.13.3. дополнен обязанностью Участника, привлеченного Расчетного центра при выявлении инцидентов обеспечить реализацию восстановления штатного функционирования объектов информационной инфраструктуры.</p> <p>9. Приложение 7 к Правилам Платежной системы, пункт 4.1. дополнено определение риска информационной безопасности.</p>
05 октября 2022 года	Редакция № 3	<p>1. Раздел «Термины и определения», пункт «Услуги платежной системы «Хелло» дополнен подпунктом «ж) от юридических лиц юридическим лицам при предоставлении полных реквизитов платежа»</p> <p>2. Раздел 7.2 «Мероприятия по управлению рисками» дополнен следующими пунктами:</p>

		<p>7.2.16 В рамках системы управления рисками в Системе Оператор Системы дополнительно определяет мероприятия, которые обязаны выполнять Участники – операторы по переводу денежных средств и операторы УПИ:</p> <ul style="list-style-type: none"> • управление риском ИБ, в качестве субъекта Системы, как одним из видов операционного риска; • установление состава показателей уровня риска ИБ в Системе (Оператор Системы рекомендует устанавливать минимум два показателя: количество инцидентов нарушения информационной безопасности и размер убытков от инцидентов риска информационной безопасности); • реализация процессов выявления и идентификации риска ИБ в Системе в отношении объектов информационной инфраструктуры участников Системы, операторов УПИ, задействованных при функционировании в Системе, включающие в себя следующие способы, но не ограничиваясь (в случае применимости): <ul style="list-style-type: none"> - анализ базы событий операционного риска, включающей события риска ИБ (далее База событий); - проведение ежегодной самооценки уровня операционного риска, включающего риск ИБ, и форм (способов) контроля, направленных на снижение его уровня, на основе формализованных анкет; - анализ динамики количественных показателей, направленных на измерение и контроль уровня операционного риска, включающего риск ИБ, в определенный момент времени (ключевых индикаторов риска); - анализ информации работников организации, полученной в рамках инициативного информирования работниками организации Службы управления рисками и (или) Службы внутреннего аудита; - анализ других внешних и внутренних источников информации и способов выявления рисков. <p>Результаты процедуры идентификации риска ИБ используются для проведения процедур количественной и качественной оценки уровня риска ИБ и корректного учета связи идентифицированного риска ИБ с событиями риска в Базе событий. Порядок ведения Базы событий подлежит определению во внутренних документах организации.</p> <p>7.2.16.1 В целях выявления и идентификации рисков ИБ процессы выявления и идентификации рисков ИБ должны быть направлены на идентификацию событий, действий, условий, которые могут оказать влияние на информационные системы и бизнес-процессы, реализующие платежные услуги, операционные услуги, услуги платежного клиринга и/или расчетные услуги в рамках Системы, а также определение возможных последствий, анализ причин и источников возникновения событий рисков ИБ.</p> <p>Выявление и анализ риска ИБ в Системе должен включать в себя:</p>
--	--	--

		<ul style="list-style-type: none"> • определение источников риска и событий (определение угроз информационной безопасности), реализация которых может привести к возникновению инцидента (риск-события), и определение для каждого из выявленных риск-событий величины риска, характеризующего вероятностью наступления риск-событий и величиной возможных последствий их реализации; • тестирования на проникновение в информационную инфраструктуру Участников, при тестировании каждой области оценивается возможность по компрометации безопасности ИТ систем Участников; • использование специализированного программного обеспечения для выявления уязвимостей программного обеспечения; • непрерывный мониторинг событий ИБ. <p>7.2.16.2 В целях минимизации последствий от реализации угроз информационной безопасности должны быть разработаны процессы реагирования на инциденты, в т.ч. планы восстановления штатного функционирования объектов информационной инфраструктуры. Процесс реагирования на инциденты защиты информации состоит из следующих последовательных этапов:</p> <ul style="list-style-type: none"> • локализация инцидента; • выявление последствий инцидента; • ликвидация последствий инцидента, • проверка работоспособности элементов, подвергшихся воздействию инцидента. <p>Основными целями процесса реагирования на инциденты являются:</p> <ul style="list-style-type: none"> • не допустить или минимизировать последствия инцидента, сохраняя непрерывность деятельности в рамках Системы; • обеспечить эффективное и своевременное восстановление работоспособности (штатного функционирования) информационных ресурсов; • повысить уровень обеспечения информационной безопасности в организации и эффективность ведения деятельности по управлению инцидентами; • реализация взаимодействия при обмене информацией об инцидентах защиты информации; • анализ возникших нештатных ситуаций и их последствий; • принятие мер по недопущению их повторного возникновения инцидента. <p>7.2.16.3 Оператор Системы в целях управления рисками осуществляет следующие мероприятия:</p> <ul style="list-style-type: none"> • определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Участниками требований к управлению рисками, установленных Правилами Системы; • определение подразделения Оператора Платежной Системы, обеспечивающие информационную безопасность, осуществляющее управление риском информационной
--	--	---

		<p>безопасности Оператора Платежной Системы в целом в т.ч. анализирующие и оценивающие обеспечение защиты информации в Платежной Системе;</p> <ul style="list-style-type: none"> • определение подразделения, осуществляющее эксплуатацию информационных систем Оператора Платежной Системы в целом, в том числе в функции которого входит обеспечение бесперебойности функционирования Оператора Платежной Системы в целом; • определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений Оператора Системы; • доведение до органов управления Оператора Системы соответствующей информации о рисках; • определение показателей бесперебойности функционирования Системы; • определение порядка обеспечения бесперебойности функционирования Системы; • определение методик анализа рисков в Системе, включая профили рисков; • определение порядка обмена информацией, необходимой для управления рисками; • определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; • определение порядка изменения операционных и технологических средств и процедур; • определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией; • определение порядка обеспечения защиты информации в Системе; • определение системы управления риском информационной безопасности Оператора Системы в целом, включая выполняемые им функции оператора УПИ. <p>7.2.16.4 Участники ПС реализуют процессы выявления, идентификации и анализа рисков информационной безопасности в отношении своих объектов информационной инфраструктуры, включая процессы реагирования на инциденты связанные с защитой информации и восстановления их штатного функционирования.</p> <p>7.2.17 Участники и привлеченные Операторы УПИ обязаны выявлять Инциденты при оказании УПИ, связанные с приостановлением их оказания и восстановлением оказания УПИ, соответствующего требованиям к оказанию услуг, в случае нарушения указанных требований и предоставлять сведения о выявленных Инцидентах Оператору ПС в течение 12 (Двенадцати) часов с момента возникновения (выявления) Инцидента путем направления сообщения по Согласованным каналам связи. Форма предоставления сведений по выявленным Инцидентам приведена в Приложении 9 к настоящим Правилам.</p> <p>7.2.18 Оператор ПС при выявлении нарушения порядка обеспечения БФПС Участниками или привлеченными Операторами УПИ:</p> <ul style="list-style-type: none"> • информирует Участников и привлеченных Операторов УПИ о выявленных в их деятельности нарушениях путем направления по Согласованным каналам связи официального письма и устанавливает сроки устранения нарушений;
--	--	--

		<ul style="list-style-type: none"> • при необходимости совместно с Участником или привлеченным Оператором УПИ согласовывает мероприятия по устранению нарушений; • осуществляет проверку результатов устранения нарушений и информирует о результатах проведенной проверки Участников и привлеченных Операторов УПИ, в деятельности которых выявлены нарушения, путем направления по Согласованным каналам связи официального письма. <p>7.2.19 При выявлении фактов неисполнения порядка обеспечения БФПС или неисполнения мероприятий по устранению выявленных нарушений привлеченными Операторами УПИ/Участниками Оператор ПС вправе приостановить участие такого Участника в Платежной системе или расторгнуть договор с привлеченным Оператором УПИ.</p> <p>7.2.20 В случаях временного приостановления (прекращения) оказания ОУПИ Оператор ПС:</p> <ul style="list-style-type: none"> • в день приостановления (прекращения) оказания УПИ информирует: <ul style="list-style-type: none"> - Банк России (Департамент национальной платежной системы) — путем направления уведомления о приостановлении (прекращении) оказания услуг платежной инфраструктуры - по адресу электронной почты: SVC_DNPS_UONN@cbr.ru с подтверждением отправки по телефонам: 8 (495) 676-86-64, 8 (495) 771-49-25; - Участников и привлеченных Операторов УПИ (в случае их привлечения) — путем направления уведомлений по Согласованным каналам связи и (или) посредством размещения уведомления на Сайте Платежной системы в информационно-телекоммуникационной сети Интернет в течение 2 (Двух) рабочих дней со дня приостановления (прекращения) оказания - ОУПИ направляет в Банк России (Департамент национальной платежной системы) уведомление на бумажном носителе или в виде электронного сообщения, снабженного Кодом аутентификации. <p>7.2.21 Определение порядка взаимодействия Субъектов ПС в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев. При возникновении спорных и чрезвычайных ситуаций Участники и привлеченные Операторы УПИ (в случае их привлечения) незамедлительно информируют Оператора ПС о данных ситуациях, о причинах их возникновения и последствиях любым доступным Участнику способом, в т.ч. путем направления сообщения в свободном формате по Согласованным каналам связи. Допускается информирование Участником и привлеченным Оператором УПИ Оператора ПС о причинах возникновения спорной/чрезвычайной ситуации, если их выявление потребует проведение отдельного расследования, по завершении такого расследования по Согласованным каналам связи, но не позднее 5 (Пяти) рабочих дней с момента возникновения спорной/чрезвычайной ситуации.</p> <p>7.2.22 Оператор ПС после получения информации в соответствии с п. 7.2.17 настоящих Правил определяет действия Участника(ов) и привлеченных Операторов УПИ с целью</p>
--	--	---

		<p>урегулирования ситуации. Конкретные действия определяются индивидуально по каждому обращению по договоренности Сторон.</p> <p>7.2.23 В случае принятия решения о модернизации или замене используемых операционных и технологических средств и процедур Оператор ПС:</p> <ul style="list-style-type: none">• разрабатывает технические требования на создание и внедрение новых операционных и технологических средств и процедур;• по завершении разработки производит тестирование новых операционных и технологических средств и процедур;• осуществляет внедрение новых операционных и технологических средств и процедур. <p>Информирование Участников о предполагаемых изменениях операционных и технологических средств и процедур Платежной системы осуществляется Оператором ПС путем публикации информации на Сайте Платежной системы с описанием планируемых изменений и сроков их внедрения. Срок, отведенный для ознакомления и направления замечаний и предложений по планируемым изменениям, устанавливается Оператором ПС, но не может быть менее 1 (Одного) месяца</p> <p>3. Раздел 7.4 «Методика анализа рисков» дополнен следующими пунктами:</p> <p>7.4.8. Идентификация рисков осуществляется ОПДС и ОУПИ путем определения их видов и источников возникновения. Идентификация каждого события риска включает в себя определение:</p> <ul style="list-style-type: none">• типа (вида) события риска;• причины (источника) события риска;• объекта события риска (вид деятельности / бизнес-процесс / документ);• места возникновения события риска;• типов возможных убытков по выявленным событиям риска. <p>7.4.9 Анализ рисков, предусматривает определение метода их измерения, определение вероятности наступления таких рисков и степени их воздействия на работоспособность ОИИ. В ходе анализа рисков делаются выводы об объектах риска, в которых реализованы/могут быть реализованы наибольшие риски (по частоте возникновения событий риска и по их тяжести (величине и существенности убытков), формулируются выводы о причинах/возможных причинах возникновения событий риска, а также выделяются факторы, приводящие к реализации риска. Анализ рисков осуществляется по каждому из видов риска, а также по совокупности рисков, реализация которых может быть взаимосвязана. Методика оценки событий рисков разрабатывается на основе как количественных, так и качественных методов. Методы качественной оценки используются в случаях, когда невозможно получить достаточно надежные данные, требуемые для количественной оценки, либо получение и анализ таких данных оказываются слишком дорогостоящими. В отношении каждого из видов рисков определяется методология оценки риска, включая набор и источники данных, используемых для оценки. На</p>
--	--	---

		<p>основе статистики реализации событий риска и его влияния на деятельность Платежной системы осуществляется определение вероятности возникновения событий риска и количественная оценка их возможных последствий (степени воздействия). Вероятностные методы оценки используются по мере накопления необходимой статистики событий соответствующего риска.</p> <p>7.4.10 Способами выявления рисков в отношении объектов информационной инфраструктуры (ОИИ) ОПДС и ОУПИ могут быть:</p> <ul style="list-style-type: none"> • проведение тестирования на проникновение и анализ уязвимостей на объектах информационной инфраструктуры, задействованных для работы в Системе не реже одного раза в год; • проведение внешнего аудита на соответствие применяемых мер по защите информации требованиям, определенным для ОПДС и ОУПИ в соответствии с положением Банка России от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств; <p>7.4.11 Информирование Оператора о выявленных в Системе рисков, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется по по согласованным каналам связи.</p> <p>4. Добавлено Приложение № 9 к Правилам Платежной системы «ХЕЛЛО» «Сведения о выявленных Инцидентах, связанных с нарушением бесперебойности функционирования Платежной системы»</p>
--	--	--