УТВЕРЖДЕНО
Решением Правления
ООО РНКО «Единая касса»
(Протокол №8 от 03.04.2024)

Председатель Правления

_____ Путинцев Е.М.

Требования к взаимодействию с субъектами национальной платежной системы ООО РНКО «Единая касса»

Версия 2.0

г. Москва

2024 г.

Реквизиты внутреннего нормативного документа	
Владелец процесса (наименование подразделения, должности, ФИО)	Служба информационной безопасности
Владелец ВНД (наименование подразделения, должности, ФИО)	СИБ, Заместитель Председателя Правления – Руководитель СИБ, Ситников А.Н.
Разработчик (наименование подразделения, должности, ФИО)	СИБ, Заместитель Председателя Правления – Руководитель СИБ, Ситников А.Н.
Изменения к документу (Изменение или новая версия (редакция))	Новая версия
№, месяц, год	Версия 2.0 апрель 2024г.
Информация о внесенных изменениях (краткое описание основных внесенных изменений)	Заменены ссылки на Положения Банка России и приказы ФСТЭК, изменены таблицы, содержащие технологические меры защиты информации.
Причина внесения изменений	Приведение в соответствие Положению Банка России № 821-П.
Предыдущие редакции документа (предыдущие версии (редакции) или все изменения, внесенные в документ)	Версия 1.0
№ протокола, дата принятия	протокол Правления №4 от 21.02.2024

Оглавление

1. Термины и определения

1.1. В настоящих Требованиях применяются следующие термины и определения:

Авторизация – проверка, подтверждение и предоставление прав логического доступа при осуществлении субъектами доступа логического доступа.

Аутентификация – проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Банковский платежный агент (БПА) - юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются кредитной организацией в целях осуществления отдельных банковских операций.

Банковский платежный субагент (БПСА) - юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются банковским платежным агентом в целях осуществления отдельных банковских операций.

Взаимная двухсторонняя аутентификация – процесс одновременной аутентификации двух сторон в рамках используемого протокола.

Двухфакторная аутентификация – аутентификация, для осуществления которой используются два различных фактора аутентификации.

Идентификация – присвоение для осуществления логического доступа субъекту (объекту) доступа уникального признака (идентификатора); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов.

Инцидент защиты информации – одно или серия связанных нежелательных или неожиданных событий защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов, технологических процессов РНКО и (или) нарушить безопасность информации.

Компенсирующие меры – меры защиты информации, направленные на нейтрализацию угроз безопасности информации, определенных в модели угроз и нарушителей безопасности информации финансовой организации.

Контур безопасности – совокупность объектов информатизации, определяемая областью применения стандарта ГОСТ Р 57580.1–2017, используемых для реализации бизнес-процессов и (или) технологических процессов финансовой организации единой степени критичности (важности), для которой финансовой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации).

Меры защиты информации – организационные (в том числе управленческие) и технические меры, применяемые для защиты информации и обеспечения доступности АС.

Объекты информационной инфраструктуры – автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, эксплуатация и использование которых обеспечивается при осуществлении переводов денежных средств.

Оператор по переводу денежных средств - организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

Оператор услуг информационного обмена (ОУИО) - организация, оказывающая операторам по переводу денежных средств на основании договоров услуги обмена информацией при осуществлении операций с использованием электронных средств платежа между операторами по переводу денежных средств и их клиентами и (или) между операторами по переводу денежных средств и иностранными поставщиками платежных услуг (далее - услуги информационного обмена). При этом оператором услуг информационного обмена не являются операционный центр и оператор связи.

Оценка соответствия – способ проверки соответствия защиты информации, включающий в себя оценку выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1.

Перевод денежных средств - действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.

Поставщик платежного приложения (ППП) - юридическое лицо, в том числе иностранная организация, предоставляющее на основании договора с оператором по переводу денежных средств платежное приложение для его применения клиентами оператора по переводу денежных средств.

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

Тестирование на проникновение и анализ уязвимостей[1] – основной метод оценки защищенности, охватывающий все аспекты функционирования подсистемы ИБ критичной системы, обеспечивающий основной бизнес-функционал организации, включая

[1] Рекомендации к проведению оценки защищенности приведены в документе «Рекомендации в области стандартизации Банка России РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» (приняты и введены в действие распоряжением Банка России от 10 июля 2014 г. N Р-556).

действия персонала по реагированию на инциденты ИБ и противодействие компьютерным атакам.

Технологические участки – участки информационной инфраструктуры организации, обеспечивающие обработку защищаемой информации. Перечень технологических участков:

1) идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;

2) формирование (подготовка), передача и прием электронных сообщений;

3) удостоверение права клиентов распоряжаться денежными средствами;

4) осуществление банковской операции, учет результатов ее осуществления;

5) хранение электронных сообщений и информации об осуществленных банковских операциях.

Сертификация – процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме, что продукция соответствует установленным требованиям (см. Закон РФ от 10 июня 1993 г. № 5151-I «О сертификации продукции и услуг»).

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Сокращения

2.1 В настоящих требованиях используются следующие сокращения:

АС – автоматизированная система;

ИАА (технологический участок) – идентификация, аутентификация и авторизация клиентов операторов по переводу денежных средств при совершении действий в целях осуществления операций по переводу денежных средств.

ИБ – информационная безопасность;

ОУ (технологический участок) – осуществление операций по переводу денежных средств, учет результатов их осуществления.

ОУД – оценочный уровень доверия;

ПО – программное обеспечение;

ППО – прикладной программное обеспечение;

РНКО – ООО РНКО «Единая касса»;

СВТ – средство вычислительной техники;

СКЗИ – средство криптографической защиты информации;

УП (технологический участок) – удостоверение права клиентов операторов по переводу денежных средств распоряжаться денежными средствами.

УЭП – усиленная электронная подпись;

ФПП (технологический участок) – формирование (подготовка), передача и прием электронных сообщений.

ХИ (технологический участок) – хранение электронных сообщений и информации об осуществленных переводах денежных средств.

ЭП – электронная подпись;

ЭС – электронное сообщение (в контексте 161-ФЗ).

3. Нормативные ссылки

3.1 Настоящие Требования разработаны с учетом и во исполнение следующих документов:

3.1.1 Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (далее – **161-ФЗ**).

3.1.2 Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – **63-ФЗ**).

3.1.3 Положение Банка России от 17 августа 2023 г. № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – **821-П**);

3.1.4 Политика информационной безопасности РНКО;

3.1.5 ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее – **ГОСТ Р 57580.1–2017**).

3.1.6 Национальный стандарт Российской Федерации ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (далее – **ГОСТ Р 57580.2–2018**).

3.1.7 Стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года N 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014) (далее - **ГОСТ Р ИСО/МЭК 15408-3-2013**).

3.1.8 Методические рекомендации Банка России от 2 ноября 2022 г. № 12-МР «По расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации» (далее – **12-МР**).

3.1.9 Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (утв. приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 г. № 76) (далее – **Приказ ФСТЭК №76**).

4. Общие сведения

4.1. Настоящие Требования являются документом, разработанным и утвержденным РНКО в целях:

4.1.1 Контроля за соблюдением БПА, в том числе БПА, осуществляющими операции платежного агрегатора, требований к защите информации при осуществлении переводов денежных средств в соответствии с заключенными договорами между РНКО и БПА, в том числе БПА, осуществляющими операции платежного агрегатора.

4.1.2 Контроля за соблюдением ОУИО требований к защите информации при предоставлении услуг информационной обмена в соответствии с заключенными договорами между РНКО и ОУИО.

4.1.3 Определения критериев необходимости и периодичности тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, проведения оценки соответствия защиты информации, сертификации или оценки соответствия прикладного ПО АС и приложений.

4.1.4 Выполнения требований 821-П и Политики информационной безопасности РНКО.

5. Требования к поставщикам платежных приложений

5.1. При привлечении РНКО поставщиков платежных приложений, предоставляющих платежные приложения для их применения клиентами РНКО, ППП должны обеспечить сертификацию[2] или оценку[3] соответствия ППО АС и приложений по требованиям к ОУД не ниже, чем ОУД 4 в соответствии с требованиями национального стандарта ГОСТ Р ИСО/МЭК 15408-3-2013.

6. Требования к банковским платежным агентам (субагентам)

6.1. БПА, в том числе БПА, осуществляющие операции платежного агрегатора, привлекаемые РНКО в целях осуществления отдельных банковских операций, определенных соответствующими договорами, обязаны:

6.1.1 Обеспечить реализацию минимального уровня защиты информации[4] для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1–2017.

6.1.2 Обеспечить проведение оценки соответствия защиты информации не реже *одного раза в два года*.

6.1.3 Обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2–2018.

6.1.4 Обеспечить проведение тестированияе на проникновение[5] и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры контура безопасности не реже *одного раза в год*. По решению БПА тестирование на проникновение и анализ уязвимостей объектов информатизации контура безопасности проводится самостоятельно или с привлечением проверяющей организации.

6.1.5 Обеспечить сертификацию[6] или оценку[7] соответствия ППО АС и приложений по требованиям к ОУД не ниже, чем ОУД 4 в соответствии с требованиями национального стандарта ГОСТ Р ИСО/МЭК 15408-3-2013, удовлетворяющего следующим критериям:

---

[2] В случае принятия решения о необходимости проведения сертификации ППО АС и приложений БПА должны обеспечить сертификацию не ниже 6 уровня доверия в соответствии с Приказом ФСТЭК № 76.

[3] По решению поставщика платежного приложения оценка ППО АС и приложений проводится самостоятельно или с привлечением проверяющей организации.

[4] В случае, если уровень защиты информации БПА был повышен в соответствии с результатом анализа рисков – необходимо обеспечивать установленный уровень защиты информации.

[5] В данном случае понимается внешнее и внутреннее тестирование на проникновение контура безопасности в рамках стандарта ГОСТ Р 57580.1–2017.

[6] В случае принятия решения о необходимости проведения сертификации ППО АС и приложений БПА должны обеспечить сертификацию не ниже 6 уровня доверия в соответствии с Приказом ФСТЭК № 76.

[7] По решению БПА оценка ППО АС и приложений проводится самостоятельно или с привлечением проверяющей организации.

a. ППО АС и приложений, распространяемое клиентам РНКО для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;

b. ПО, эксплуатируемого на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде (электронные сообщения), к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет».

6.1.6 Обеспечить реализацию технологических мер по обеспечению защиты информации, в соответствии с Приложением 1 к настоящим Требованиям и Приложением 2 к 821-П.

6.1.7 Информировать РНКО в случаях выявления инцидентов, перечень которых приведен в Приложении 3 к настоящим Требованиям. Информация об инциденте передаётся в произвольном виде на адрес электронной почты Службы информационной безопасности РНКО (oib@w1.money). Информация должна содержать:

– Дату и время выявления инцидента;

– Дату и время возникновения инцидента (если известно);

– Описание инцидента (кратко описывается инцидент с указанием нарушителя (если известно), хронология инцидента, механизм реализации инцидента, перечень ресурсов, на которые был направлен инцидент, возможные цели нарушителя, недостатки (уязвимости), ставшие причиной инцидента);

– Все выявленные последствия инцидента;

– Оценка размера реального ущерба от инцидента;

– Описание и результаты выполненных действий по нейтрализации инцидента и устранению его последствий.

6.1.8 В случае обработки данных пластиковых карт пользователей выполнять требования действующей редакции стандарта PCI Data Security Standard (PCI DSS).

7. Требования к банковским платежным агентам, осуществляющим операции платежного агрегатора

7.1 БПА, осуществляющие операции платежного агрегатора, привлекаемы РНКО в целях осуществления отдельных банковских операций, определенных соответствующими договорами, обязаны:

7.1.1. Обеспечить реализацию минимального уровня защиты информации[8] для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1–2017.

7.1.2 Обеспечить проведение оценки соответствия защиты информации не реже *одного раза в два года*.

7.1.3 Обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2–2018.

7.1.4 Обеспечить проведение тестирования[9] на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры контура безопасности не реже *одного раза в год*. По решению БПА, осуществляющих операции платежного агрегатора, тестирование на проникновение и анализ уязвимостей объектов информатизации контура безопасности проводится самостоятельно или с привлечением проверяющей организации.

7.1.5 Обеспечить сертификацию[10] или оценку[11] соответствия прикладного программного обеспечения автоматизированных систем и приложений по требованиям к ОУД не ниже, чем ОУД 4 в соответствии с требованиями национального стандарта ГОСТ Р ИСО/МЭК 15408-3-2013, удовлетворяющего следующим критериям:

a. ППО АС и приложений, распространяемое клиентам РНКО для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;

b. ПО, эксплуатируемого на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде (электронные сообщения), к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет».

---

[8] В случае, если уровень защиты информации БПА, осуществляющих операции платежного агрегатора, был повышен в соответствии с результатом анализа рисков – необходимо обеспечивать установленный уровень защиты информации.

[9] В данном случае понимается внешнее и внутреннее тестирование на проникновение.

[10] В случае принятия решения о необходимости проведения сертификации ППО АС и приложений БПА, осуществляющие операции платежного агрегатора, должны обеспечить сертификацию не ниже 6 уровня доверия в соответствии с Приказом ФСТЭК № 76.

[11] По решению БПА, осуществляющих операции платежного агрегатора, оценка ППО АС и приложений проводится самостоятельно или с привлечением проверяющей организации.

7.1.6 Обеспечить реализацию технологических мер по обеспечению защиты информации в соответствии с Приложением 1 к настоящим Требованиям и Приложением 2 к 821-П.

7.1.7 Информировать РНКО в случаях выявления инцидентов, перечень которых приведен в Приложении 3 к настоящим Требованиям. Информация об инциденте передаётся в произвольном виде на адрес электронной почты Службы информационной безопасности РНКО (oib@w1.money). Информация должна содержать:

– Дату и время выявления инцидента;

– Дату и время возникновения инцидента (если известно);

– Описание инцидента (кратко описывается инцидент с указанием нарушителя (если известно), хронология инцидента, механизм реализации инцидента, перечень ресурсов, на которые был направлен инцидент, возможные цели нарушителя, недостатки (уязвимости), ставшие причиной инцидента);

– Все выявленные последствия инцидента;

– Оценка размера реального ущерба от инцидента;

– Описание и результаты выполненных действий по нейтрализации инцидента и устранению его последствий.

7.1.8 В случае обработки данных пластиковых карт пользователей выполнять требования действующей редакции стандарта PCI Data Security Standard (PCI DSS).

8. Требования к операторам услуг информационного обмена

8.1. ОУИО, привлекаемые РНКО на основании договоров услуги обмена информации при осуществлении операций с использованием электронных средств платежа между РНКО и клиентами, обязаны:

8.1.1 Обеспечить реализацию стандартного[12] уровня защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1–2017.

8.1.2 Обеспечить проведение оценки соответствия защиты информации не реже *одного раза в два года*.

8.1.3 Обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2–2018.

8.1.4 Обеспечить проведение тестирования[13] на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры контура безопасности не реже *одного раза в год*. По решению ОУИО тестирование на проникновение и анализ уязвимостей объектов информатизации контура безопасности проводится самостоятельно или с привлечением проверяющей организации.

8.1.5 Обеспечить сертификацию или проведение оценки[14] соответствия по требованиям к ОУД[15] не нижем чем ОУД 4, в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 в отношении ППО АС и приложений, удовлетворяющего следующим критериям:

a. ППО АС и приложений, распространяемое клиентам РНКО для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;

b. ПО, эксплуатируемого на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде (электронные сообщения), к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет».

[12] По решению ОУИО уровень защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1–2017 может быть повышен на основе анализа рисков.

[13] В данном случае понимается внешнее и внутреннее тестирование на проникновение.

[14] По решению ОУИО, оценка ППО АС и приложений проводится самостоятельно или с привлечением проверяющей организации.

[15] В случае принятия решения о проведении сертификации прикладного программного обеспечения автоматизированных систем и приложений операторы услуг информационного обмена должны обеспечить сертификацию не ниже 5 уровня доверия в соответствии с Приказом ФСТЭК № 76.

8.1.6 Обеспечить реализацию технологических мер по обеспечению защиты информации в соответствии с Приложением 1 к настоящим Требованиям и Приложением 2 к 821-П.

8.1.7 Информировать РНКО в случаях выявления инцидентов, перечень которых приведен в Приложении 3 к настоящим Требованиям. Информация об инциденте передаётся в произвольном виде на адрес электронной почты Службы информационной безопасности РНКО (oib@w1.money). Информация должна содержать:

– Дату и время выявления инцидента;

– Дату и время возникновения инцидента (если известно);

– Описание инцидента (кратко описывается инцидент с указанием нарушителя (если известно), хронология инцидента, механизм реализации инцидента, перечень ресурсов, на которые был направлен инцидент, возможные цели нарушителя, недостатки (уязвимости), ставшие причиной инцидента);

– Все выявленные последствия инцидента;

– Оценка размера реального ущерба от инцидента;

– Описание и результаты выполненных действий по нейтрализации инцидента и устранению его последствий.

8.1.8 В случае обработки данных пластиковых карт пользователей выполнять требования действующей редакции стандарта PCI Data Security Standard (PCI DSS).

9. Требования к предоставлению свидетельств банковскими платежными агентами

9.1. В рамках подтверждения реализации требований к защите информации, установленных в 821-П к БПА, в том числе БПА, осуществляющим операции платежного агрегатора, РНКО устанавливает следующие требования к предоставлению свидетельств:

9.1.1 В части реализации пунктов 6.1.1–6.1.3 настоящих Требований и формирования отчета оценки соответствия БПА – предоставить *в течение 30 дней с момента проведения* оценки соответствия требований к защите информации по ГОСТ Р 57580.1–2017 результаты по форме, представленной в методических рекомендациях Банка России 12-МР.

9.1.2 В части реализации пункта 6.1.4 настоящих Требований БПА необходимо предоставить результаты проведения тестирования на проникновение и план закрытия выявленных критичных уязвимостей – по запросу РНКО или *не позднее 30 дней с момента проведения*.

9.1.3 В части реализации пункта 6.1.5 настоящих Требований БПА необходимо предоставить сертификаты, подтверждающие соответствие требований к ОУД не ниже, чем ОУД 4 или результаты проведения сертификации ППО АС и приложений не ниже 6 уровня доверия, в соответствии с Приказом ФСТЭК № 76 – по запросу РНКО или *не позднее 30 дней с момента проведения*.

9.1.4 В части реализации пункта 6.1.6 настоящих Требований БПА необходимо предоставить результаты выполнения требований технологических мер по обеспечению защиты информации, в соответствии с Приложением 1 к настоящим Требованиям и Приложения 2 к 821-П – по запросу РНКО или *не позднее 30 дней с момента проведения*.

9.1.5 В случае обработки данных пластиковых карт пользователей - ежеквартально предоставлять результаты ASV сканирования и план по закрытию уязвимостей (в случае обнаружения).

9.1.6 В случае обработки данных пластиковых карт пользователей ежегодно предоставлять результаты ежегодного сертификационного аудита с привлечением QSA аудитора или результаты ежегодной самооценки (при обработке менее 300 000 операций в год) – по запросу РНКО или *не позднее 30 дней с момента проведения*.

10. Требования к предоставлению свидетельств банковскими платежными агентами, осуществляющими операции платежного агрегатора

10.1. В рамках подтверждения реализации требований к защите информации, установленных в 821-П к БПА, осуществляющим операции платежного агрегатора, РНКО устанавливает следующие требования к предоставлению свидетельств:

10.1.1 В части реализации пунктов 7.1.1–7.1.3 настоящих Требований БПА, осуществляющим операции платежного агрегатора, необходимо предоставить *в течение 30 дней с момента подписания отчета* о результатах проведения оценки соответствия требованиям стандарта ГОСТ Р 57580.1–2017, по форме, представленной в методических рекомендациях Банка России 12-МР.

10.1.2 В части реализации пункта 7.1.4 настоящих Требований БПА, осуществляющим операции платежного агрегатора, необходимо предоставить результаты проведения тестирования на проникновение и план закрытия выявленных критичных уязвимостей – по запросу РНКО или *не позднее 30 дней с момента проведения*.

10.1.3 В части реализации пункта 7.1.5 настоящих Требований БПА, осуществляющим операции платежного агрегатора, необходимо предоставить сертификаты, подтверждающие соответствие требований к ОУД не ниже, чем ОУД 4, или результаты проведения сертификации ППО АС и приложений не ниже 6 уровня доверия, в соответствии с Приказом ФСТЭК № 76 – по запросу РНКО или *не позднее 30 дней с момента проведения*.

10.1.4 В части реализации пункта 7.1.6 настоящих Требований БПА, осуществляющим операции платежного агрегатора, необходимо предоставить результаты выполнения требований технологических мер по обеспечению защиты информации, в соответствии с Приложением 1 к настоящим Требованиям и Приложения 2 к 821-П – по запросу РНКО или *не позднее 30 дней с момента проведения*.

10.1.5 В части реализации пункта 7.1.7 настоящих Требований БПА, осуществляющим операции платежного агрегатора, необходимо предоставить результаты выполнения требований технологических мер по обеспечению защиты информации, в соответствии с Приложением 1 к настоящим Требованиям и Приложения 2 к 821-П – по запросу РНКО или *не позднее 30 дней с момента проведения*.

10.1.6 В случае обработки данных пластиковых карт пользователей - ежеквартально предоставлять результаты ASV сканирования и план по закрытию уязвимостей (в случае обнаружения).

10.1.7 В случае обработки данных пластиковых карт пользователей ежегодно предоставлять результаты ежегодного сертификационного аудита с привлечением QSA аудитора или результаты ежегодной самооценки (при обработке менее 300 000 операций в год) – по запросу РНКО или *не позднее 30 дней с момента проведения*.

11. Требования к предоставлению свидетельств операторами услуг информационного обмена

11.1. В рамках подтверждения реализации требований к защите информации, установленных в 821-П к ОУИО, РНКО устанавливает следующие требования к предоставлению свидетельств:

11.1.1 В части реализации пунктов 8.1.1–8.1.3 настоящих Требований ОУИО необходимо предоставить *в течение 30 дней с момента подписания* отчета о результатах проведения оценки соответствия требованиям стандарта ГОСТ Р 57580.-2017, по форме, представленной в методических рекомендациях Банка России 12-МР.

11.1.2 В части реализации пункта 8.1.4 настоящих Требований ОУИО необходимо предоставить результаты проведения тестирования на проникновение и план закрытия выявленных критичных уязвимостей – по запросу РНКО или *не позднее 30 дней с момента проведения*.

11.1.3 В части реализации пункта 8.1.5 настоящих Требований ОУИО необходимо предоставить сертификаты, подтверждающие соответствие требований к ОУД не ниже, чем ОУД 4, или результаты проведения сертификации ППО АС и приложений не ниже 5 уровня доверия, в соответствии с Приказом ФСТЭК № 76 – по запросу РНКО или *не позднее 30 дней с момента проведения*.

11.1.4 В части реализации пункта 8.1.6 настоящих Требований ОУИО необходимо предоставить результаты выполнения требований технологических мер по обеспечению защиты информации, в соответствии с Приложением 1 к настоящим Требованиям и Приложения 2 к 821-П – по запросу РНКО или *не позднее 30 дней с момента проведения*.

11.1.5 В части реализации пункта 8.1.7 настоящих Требований ОУИО необходимо предоставить результаты выполнения требований технологических мер по обеспечению защиты информации, в соответствии с Приложением 1 к настоящим Требованиям и Приложения 2 к 821-П – по запросу РНКО или *не позднее 30 дней с момента проведения*.

11.1.6 В случае обработки данных пластиковых карт пользователей - ежеквартально предоставлять результаты ASV сканирования и план по закрытию уязвимостей (в случае обнаружения).

11.1.7 В случае обработки данных пластиковых карт пользователей ежегодно предоставлять результаты ежегодного сертификационного аудита с привлечением QSA аудитора или результаты ежегодной самооценки (при обработке менее 300 000 операций в год) – по запросу РНКО или *не позднее 30 дней с момента проведения*.

Приложение 1

Таблица технологических мер по обеспечению защиты информации при осуществлении переводов денежных средств на технологических участках(в соответствии с Приложением 2 к 821-П)

N п/п	Операция	Защищаемая информация	Технологич. участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
Банковские платежные агенты (субагенты)															
1	Принятие от физического лица, юридического лица, индивидуального предпринимателя и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года N 161-ФЗ, наличных денежных средств, в том числе с применением платежных терминалов и банкоматов	Информация, содержащаяся в электронных сообщениях физических лиц, юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года N 161-ФЗ. Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и операторов по переводу денежных средств, в том числе в электронных сообщениях, составленных банковскими платежными агентами (субагентами) от имени операторов по переводу денежных средств. Информация, содержащаяся в реестрах, сформированных на основе электронных сообщений (далее - реестр электронных сообщений) физических лиц, юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года N 161-ФЗ. Ключевая информация СКЗИ,	ФПП	Формирование (подготовка) физическими лицами, юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 12 статьи 14 Федерального закона от 27 июня 2011 года N 161-ФЗ, электронных сообщений			+		+						
				Прием банковским платежным агентом (субагентом) электронных сообщений			+	+	+						
				Формирование(передача) банковским платежным агентом (субагентом) электронных сообщений, передача электронных сообщений в адрес операторов по переводу денежных средств			+	+		+		+	+		
				Формирование банковским платежным агентом (субагентом) реестра электронных сообщений физических лиц, юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года N 161-ФЗ.			+			+		+	+		

		используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств	ХИ	Хранение банковским платежным агентом (субагентом) электронных сообщений, обмен которыми осуществлялся при его взаимодействии с физическими лицами, юридическими лицами, индивидуальными предпринимателями, иными лицами, указанными в части 12 статьи 14 Федерального закона от 27 июня 2011 года N 161-ФЗ и операторами по переводу денежных средств									+	+
2	Выдача физическому лицу наличных денежных средств, в том числе с применением платежных терминалов и банкоматов	Информация, используемая для идентификации, аутентификации и авторизации физических лиц при осуществлении доступа к системам дистанционного банковского обслуживания. Информация, содержащаяся в электронных сообщениях физических лиц. Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и операторов по переводу денежных средств, в том числе при подтверждении права физических лиц получать наличные денежные средства. Информация об осуществленных операциях по выдаче наличных денежных средств физических лиц. Ключевая информация СКЗИ, используемая при осуществлении	ИАА	Осуществление доступа физических лиц к системам дистанционного банковского обслуживания в целях осуществления выдачи наличных денежных средств на основании запросов физических лиц	+	+									
			ФПП	Формирование (подготовка) физическими лицами электронных сообщений			+		+						
				Формирование банковским платежным агентом (субагентом) реестра электронных сообщений физических лиц			+			+		+	+		
				Прием банковским платежным агентом (субагентом) электронных сообщений			+	+	+						
				Формирование (подготовка) банковским платежным агентом (субагентом) электронных сообщений и направление электронных сообщений в адрес операторов по			+	+		+		+	+		

		обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств.		переводу денежных средств											
			УП	Получение банковским платежным агентом (субагентом) от оператора по переводу денежных средств подтверждения права физического лица получать наличные денежные средства			+	+		+	+				
			ОУ	Выдача банковским платежным агентом (субагентом) физическим лицам наличных денежных средств			+					+			
			ХИ	Хранение банковским платежным агентом (субагентом) электронных сообщений, обмен которыми осуществлялся при его взаимодействии с физическими лицами и операторами по переводу денежных средств										+	+
Банковские платежные агенты, осуществляющие операции платежного агрегатора															
3	Формирование (подготовка) электронных сообщений при обеспечении приема электронных средств платежа юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 13 статьи 14 [1] Федерального закона N 161-ФЗ, при	Информация, содержащаяся в электронных сообщениях при обеспечении приема электронных средств платежа банковскими платежными агентами, осуществляющими операции платежного агрегатора. Информация, содержащаяся в электронных сообщениях, направляемых банковскими платежными агентами, осуществляющими операции платежного агрегатора, операторам по переводу денежных средств, операторам услуг информационного обмена. Информация, содержащаяся в реестрах электронных сообщений при	ФПП	Формирование банковским платежным агентом, являющимся платежным агрегатором, электронных сообщений, передача и прием банковским платежным агентом, осуществляющим операции платежного агрегатора, сформированных электронных сообщений			+	+	+			+	+		
			ХИ	Хранение банковским платежным агентом, осуществляющим операции платежного агрегатора, информации об осуществленных операциях по переводу денежных средств										+	+

	участии в переводе денежных средств в пользу юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 13 статьи 14 [1] Федерального закона N 161-ФЗ, по операциям с использованием электронных средств платежа	обеспечении приема электронных средств платежа банковскими платежными агентами, осуществляющими операции платежного агрегатора. Информация об осуществленных операциях по переводу денежных средств. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами, осуществляющими операции платежного агрегатора, операторами по переводу денежных средств, операторами услуг информационного обмена.													
Операторы услуг информационного обмена																
4	Оказание услуг информационного обмена при осуществлении переводов денежных средств с использованием электронных средств платежа на основании электронных сообщений клиентов операторов по переводу денежных средств	Информация, используемая для идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при осуществлении переводов денежных средств. Информация, содержащаяся в электронных сообщениях клиентов операторов по переводу денежных средств. Информация, содержащаяся в электронных сообщениях, обмен которыми осуществляется при взаимодействии операторов услуг информационного обмена с операторами по переводу денежных средств, клиентами операторов по переводу денежных средств.	ИАА	Совершение действий, связанных с переводами денежных средств клиентами операторов по переводу денежных средств	+										
			ФПП	Формирование (подготовка) клиентом оператора по переводу денежных средств электронных сообщений, передача и прием оператором услуг информационного обмена электронных сообщений			+	+	+						
				Формирование оператором услуг информационного обмена реестра электронных сообщений клиентов операторов по переводу денежных средств			+					+	+		
			УП	Получение оператором услуг информационного обмена от			+	+		+	+				

		Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами услуг информационного обмена, операторами по переводу денежных средств, клиентами операторов по переводу денежных средств. Информация об осуществлении перевода денежных средств, содержащаяся в реестрах электронных сообщений клиентов операторов по переводу денежных средств. Информация, используемая для удостоверения права клиентов операторов по переводу денежных средств распоряжаться денежными средствами. Информация об осуществленных переводах денежных средств		оператора по переводу денежных средств подтверждения права клиента оператора по переводу денежных средств распоряжаться денежными средствами											
			ОУ	Осуществление оператором услуг информационного обмена операций, связанных с переводом денежных средств, путем обмена электронными сообщениями с операторами по переводу денежных средств, в том числе на основании реестра электронных сообщений клиентов операторов по переводу денежных средств			+	+		+		+	+		
				Получение оператором услуг информационного обмена результатов осуществления переводов денежных средств, в том числе путем обмена электронными сообщениями с операторами по переводу денежных средств			+	+		+		+			
			ХИ	Хранение оператором услуг информационного обмена электронных сообщений, обмен которыми осуществлялся при его взаимодействии с клиентами операторов по переводу денежных средств, операторами по переводу денежных средств										+	+
				Хранение оператором услуг информационного обмена результатов осуществления операций по переводам денежных средств										+	

Приложение 2

Описание и примеры реализации технологических мер защиты информации

№	Описание технологических мер по обеспечению защиты информации	Пример реализации
1	Реализация механизма идентификации, аутентификации и авторизации клиентов при совершении ими действий в целях осуществления переводов денежных средств.	Использование стандартных механизмов, не требующих примера реализации.
2	Реализация механизма двухфакторной аутентификации клиентов при совершении ими действий в целях осуществления переводов денежных средств.	Реализация технологической меры возможна, например, при помощи дополнительного подтверждения входа пользователя при помощи SMS-сообщения с кодом подтверждения или генерации OTP-кода в приложении для генерации кодов.
3	Применение механизмов и (или) протоколов формирования и обмена электронными сообщениями, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификацию входных электронных сообщений.	Реализация технологической меры возможна при помощи использования специализированных протоколов, например: 1. HTTPS. 2. TLS. При этом рекомендуется использовать инструмент https://www.ssllabs.com/ssltest/ для анализа используемых сертификатов, поддерживаемых протоколов и методов шифрования.
4	Взаимная (двухсторонняя) аутентификация участников обмена средствами вычислительной техники РНКО, банковских платежных агентов (субагентов) клиентов операторов по переводу денежных средств.	Реализация технологической меры возможна, например: 1. При помощи набора протоколов IPsec (применение сертификатов, либо предварительно распределяемых паролей); 2. При помощи использования протокола SSH, по умолчанию реализующего данное требование.
5	Использование простой или усиленной электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».	Реализация технологической меры в рамках взаимодействия пользователей ОУИО с ОУИО возможна при помощи аутентификации пользователя по паролю в ИС, обеспечивающей аутентификацию пользователя.
6	Использование усиленной электронной	Реализация технологической меры в

	подписи для контроля целостности и подтверждения подлинности электронных сообщений в соответствии с Федеральным законом № 63-ФЗ.	рамках взаимодействия ОУИО – РНКО возможна при помощи: 1. IPsec-туннеля. 2. Авторизации пользователя при помощи протокола SSH (где используется ключ-аутентификации или пароль).
7	Получение подтверждения от РНКО права клиента РНКО распоряжаться денежными средствами.	По умолчанию при помощи встроенного функционала АБС.
8	Проверка соответствия (сверка) результатов осуществления операций, связанных с переводом денежных средств, с информацией, содержащейся в электронных сообщениях.	В рамках реализации технологической меры в РНКО в сервисе должна быть предоставлена возможность отслеживания доступного остатка денежных средств (платежный лимит), просмотра и выгрузки потранзакционных реестров.
9	Реализация мер, направленных на проверку правильности формирования (подготовки) электронных сообщений (двойной контроль).	Выделение двух сегментов формирования и контроля электронных сообщений, позволяющих выполнить технологическую меру.
10	Обеспечение хранения защищаемой информации, информации о событиях, подлежащих регистрации, информации об инцидентах защиты информации в течение пяти лет с даты формирования информации в неизменном виде.	Настоящая технологическая мера может быть реализована при помощи: 1. Централизованной системы сбора событий защиты информации (SIEM-систем) и/или иной системы, обеспечивающей хранение событий защиты информации; 2. Электронного журнала учета инцидентов защиты информации (например, в электронном виде).
11	Восстановление защищаемой информации в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники.	Настоящая технологическая мера может быть реализована при помощи: 1. Регламента резервного копирования (и/или иного документа, регламентирующего аналогичные требования); 2. Использования средств резервного копирования (например, Veeam Backup Essentials).

Приложение 3

Перечень инцидентов при осуществлении переводов денежных средств

1. К инцидентам при осуществлении переводов денежных средств относятся:

1.1. несанкционированный доступ к информации;

1.2. нарушение в обеспечении защиты информации, включая нарушение работы технических мер защиты информации, появление уязвимостей защиты информации;

1.3. нарушение требований законодательства Российской Федерации, в том числе нормативных актов Банка России, внутренних документов финансовой организации в области обеспечения защиты информации;

1.4. нарушение регламентированных сроков выполнения процедур и операций в рамках предоставления финансовых услуг;

1.5. нарушение установленных показателей предоставления финансовых услуг;

1.6. нанесение финансового ущерба финансовой организации, ее клиентам и контрагентам;

1.7. выполнение операций (транзакций), приводящих к финансовым последствиям финансовой организации, ее клиентов и контрагентов, осуществление переводов денежных средств по распоряжению лиц, не обладающих соответствующими полномочиями, или с использованием искаженной информации, содержащейся в соответствующих распоряжениях (электронных сообщениях).