НКО «МОНЕТА» (ООО) ИНН 1215192632, КПП 121501001 ОГРН 1121200000316, ОКПО 38024380	УТВЕРЖДЕНО Решением Правления НКО «МОНЕТА» (ООО) Протокол № 42-25 от 11.12.2025 Вступает в силу с 12.12.2025

ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ ДЛЯ БАНКОВСКИХ ПЛАТЕЖНЫХ АГЕНТОВ, ПРИВЛЕКАЕМЫХ НКО «МОНЕТА» (ООО)

(Версия № 1.0)

Йошкар-Ола, 2025

ОГЛАВЛЕНИЕ

1. Контроль версий документа

Версия	Дата	Внесенные изменения
1.0	11.12.2025	Исходная версия.

2. Порядок пересмотра документа

2.1. Пересмотр настоящего документа проводится при возникновении следующих условий:

– в случае изменения требований к обеспечению защиты информации при осуществлении переводов денежных средств со стороны законодательства Российской Федерации, органов исполнительной власти Российской Федерации и Центрального банка Российской Федерации;

– в случае существенных изменений в процессах взаимодействия Небанковской кредитной организации «МОНЕТА» (общество с ограниченной ответственностью) с банковскими платежными агентами;

– в случае существенных изменений в системе управления рисками Небанковской кредитной организации «МОНЕТА» (общество с ограниченной ответственностью).

3. Термины и сокращения

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

НКО – Небанковская кредитная организация «МОНЕТА» (общество с ограниченной ответственностью), оператор по переводу денежных средств в соответствии с законодательством Российской Федерации.

Оценка соответствия защиты информации – процесс оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» (далее по тексту – ГОСТ Р 57580.1-2017), выполняемой проверяющей организацией.

Уровень защиты информации – определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов финансовой организации.

4. Общие положения

4.1. Настоящий документ разработан в соответствии с Положением Банка России от 17.08.2023 № 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 по тексту – 821-П) и регламентирует критерии и требования, устанавливаемые НКО, к обеспечению защиты информации при осуществлении переводов денежных средств при привлечении БПА.

4.2. Настоящий документ определяет критерии необходимости и периодичности тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, проведения оценки соответствия защиты информации, сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения для БПА, установленные НКО на основе системы управления рисками.

4.3. Установленные требования подлежат исполнению БПА начиная со второго квартала, следующего за кварталом фактического начала взаимодействия с НКО.

5. Требования к БПА

5.1. В соответствии с пунктом 1 статьи 14 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» НКО привлекает БПА для принятия от физического лица наличных денежных средств.

БПА должны реализовывать требования к защите информации в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при осуществлении операций, указанных в первом абзаце настоящего пункта (далее по тексту – объекты информационной инфраструктуры).

5.2. БПА должны обеспечивать реализацию минимального уровня защиты информации для объектов информационной инфраструктуры, предусмотренного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

5.3. Для дифференциации требований к защите информации при осуществлении переводов денежных средств НКО устанавливает уровни критичности БПА на основании следующих критериев:

– объем операций за отчетный квартал;

– количество точек БПА.

Определение уровней критичности приведено в Приложении №1 к настоящему документу.

5.4. НКО для каждого уровня критичности БПА устанавливает требования к обеспечению защиты информации в части проведения:

– оценки соответствия защиты информации;

– тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры;

– сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

Требования к обеспечению защиты информации в зависимости от уровня критичности БПА приведены в Приложении №2 к настоящему документу.

6. Контроль НКО за соблюдением БПА настоящих Требований

6.1. По запросу НКО БПА должны предоставить следующие подтверждения соблюдения требований, установленных в разделе 5 настоящего документа:

– отчет по результатам оценки соответствия защиты информации – в рамках соблюдения требований, предусматривающих достижение установленного минимального уровня итоговой оценки соответствия защиты информации;

– результаты проведения тестирования на проникновение в информационную инфраструктуру и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры – в рамках соблюдения требований, предусматривающих тестирование на проникновение в информационную инфраструктуру

и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры;

– подтверждение сертификации программного обеспечения автоматизированных систем и приложений или подтверждения оценки программного обеспечения по требованиям к оценочному уровню доверия – в рамках соблюдения требований, предусматривающих сертификацию в системе сертификации ФСТЭК или оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

Приложение №1. Определение уровня критичности БПА
в зависимости от объема операций за отчетный квартал
и количества точек БПА

Объем операций за отчетный квартал	**Количество точек БПА**		
	Менее 100	**От 100 до 500**	**Более 500**
Не превышает 80 млн. рублей	Низкий	Средний	–
Равен или превышает 80 млн. рублей	Средний	Высокий	Очень высокий

Приложение №2. Требования к обеспечению защиты информации в зависимости от уровня критичности БПА

Уровень критичности БПА	Требования к обеспечению защиты информации
Низкий	1. Проведение оценки соответствия защиты информации не реже одного раза в три года. 2. Реализация мер защиты информации, обеспечивающих достижение итоговой оценки соответствия не ниже 0,4 по результатам процедуры оценки соответствия защиты информации, предусмотренной ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (далее по тексту – ГОСТ Р 57580.2-2018).
Средний	1. Проведение оценки соответствия защиты информации не реже одного раза в два года. 2. Реализация мер защиты информации, обеспечивающих достижение итоговой оценки соответствия не ниже 0,55 по результатам процедуры оценки соответствия защиты информации, предусмотренной ГОСТ Р 57580.2-2018.
Высокий	1. Проведение оценки соответствия защиты информации не реже одного раза в два года. 2. Реализация мер защиты информации, обеспечивающих достижение итоговой оценки соответствия не ниже 0,75 по результатам процедуры оценки соответствия защиты информации, предусмотренной ГОСТ Р 57580.2-2018.
Очень высокий	1. Проведение оценки соответствия защиты информации не реже одного раза в два года. 2. Реализация мер защиты информации, обеспечивающих достижение итоговой оценки соответствия не ниже 0,85 по результатам процедуры оценки соответствия защиты информации, предусмотренной ГОСТ Р 57580.2-2018. 3. Ежегодное проведение тестирования на проникновение в информационную инфраструктуру и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры. 4. Обеспечение сертификации в системе сертификации ФСТЭК или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения по требованиям к ОУД не ниже, чем ОУД 4, предусмотренного 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».