Требования к защите информации для БПА, осуществляющих операции платежного Агрегатора.

Данные требования распространяются на банковских платежных агентов, осуществляющих операции платежного агрегатора.

I. БПА, осуществляющие операции платежного агрегатора (Агрегаторы), должны обеспечивать защиту информации:

- в процессе формирования (подготовки) электронных сообщений (ЭС) при обеспечении приема электронных средств платежа (ЭСП) юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 13 статьи 14.1 Федерального закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе" (далее – «Поставщики товаров/услуг»);
- при участии в переводе денежных средств в пользу Поставщиков товаров/услуг по операциям с использованием ЭСП.

II. **Защищаемая информация при совершении указанных в п.1 операций**:

- Информация, содержащаяся в ЭС при обеспечении Агрегатором приема ЭСП.
- Информация, содержащаяся в ЭС, направляемых Агрегатором КИВИ Банку (АО) (Банк), операторам услуг информационного обмена (здесь и далее - ОУИО, упоминаются при их наличии в технологической цепочке совершения операций).
- Информация, содержащаяся в реестрах ЭС при обеспечении приема ЭСП Агрегатором.
- Информация об осуществленных операциях по переводу денежных средств.
- Ключевая информация СКЗИ (средства криптографической защиты информации), используемая при осуществлении обмена ЭС между Агрегатором, Банком, ОУИО.

III. Агрегаторы должны **обеспечить проведение оценки соответствия защиты информации не реже одного раза в два года.**

Агрегаторы должны обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018. Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих предусмотренную законодательством лицензию.

Данное требование является общим для всех Агрегаторов, не зависит от дополнительных критериев, устанавливаемых Банком в разделе IV данных требований.

IV. В соответствии с п. 2.11. и п. 3.9. Положения 719-П Банк устанавливает следующие критерии для Агрегаторов.

Если при взаимодействии Банка и Агрегатора:

1. **Агрегатор осуществляет операции в отношении 50 и более Поставщиков товаров/услуг**

или

Требования к защите информации для БПА, осуществляющих операции платежного Агрегатора.

2. **общий объем** осуществляемых Агрегатором в отношении Поставщиков товаров/услуг операций **составляет сумму равную или превышающую 300 миллионов рублей за отчетный квартал,** то

Агрегатору **дополнительно необходимо**:

А) не реже одного раза в два года проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры,

Б) при обработке защищаемой информации **использовать программное обеспечение** автоматизированных систем и приложений и иное программное обеспечение, указанное в Положении 719-П, **прошедшее сертификацию** в системе сертификации Федеральной службы по техническому и экспортному контролю

или

осуществлять оценку соответствия указанного программного обеспечения по требованиям к оценочному уровню доверия (далее - ОУД) не ниже ОУД 4 в соответствии с требованиями национального 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".

Оценка соответствия программного обеспечения Платежного агрегатора должна осуществляться с привлечением проверяющей организации либо может быть проведена самостоятельно.

V. Агрегатору **необходимо** в течение 5 (пяти) рабочих дней с даты получения запроса от Банка, если иной срок не указан в соответствующем запросе, **предоставить в Банк**:

- отчеты по результатам проведения оценки соответствия защиты информации в соответствии с ГОСТ Р 57580.2-2018;

В случае достижения хотя бы одного из критериев, установленных в разделе IV данного документа:

- результаты проведенных тестирований на проникновение 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 не ниже, чем ОУД 4.

Предоставление указанных документов является достаточным подтверждением со стороны Агрегатора выполнения всех требований Положения 719-П.

Требования к защите информации для БПА, осуществляющих операции платежного Агрегатора.

VI. Общие требования, технологические и иные меры в соответствии с Положением 719-П:

1. В отношении защищаемой информации Агрегатор должен обеспечивать:

- целостность и достоверность защищаемой информации;

Целостность и достоверность защищаемой информации обеспечивается использованием усиленной электронной подписи для контроля целостности и подтверждения подлинности электронных сообщений в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи" (далее - Федеральный закон N 63-ФЗ).

- регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации;

Выполнение данного требования реализовывается Агрегатором с учетом масштабов и характера деятельности самостоятельно. Способы, инструменты выполнения выбираются Агрегатором самостоятельно. При этом Банк рекомендует реализовывать минимально необходимые меры:

- формировать службы информационной безопасности (иные подразделения с аналогичными функциями) или назначать должностное лицо (работника), ответственного за организацию защиты информации (далее – служба), определять во внутренних документах цели и задачи деятельности службы и выделять ресурсы для выполнения целей и задач службы;

- наделять службу полномочиями по контролю (мониторингу) технологии обработки защищаемой информации, выполнения работниками требований к обеспечению ЗИ;

- фиксировать во внутренних документах решения о необходимости применения организационных мер защиты информации и/или использования технических средств защиты, в т.ч. обеспечивать контроль предоставляемого доступа к защищаемой информации, предпринимать меры по предотвращению хищений носителей защищаемой информации.

- регистрацию результатов совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

  - прием (передача) ЭС при взаимодействии Банка и Агрегатора при осуществлении переводов денежных средств, в том числе для учета результатов переводов денежных средств;

  - реализация мер, направленных на проверку правильности формирования (подготовки) ЭС (двойной контроль);

  - осуществление доступа работников к защищаемой информации, выполняемого с использованием автоматизированных систем, программного обеспечения.

  Регистрации подлежат следующие данные о действиях, выполняемых работниками с использованием автоматизированных систем,

программного обеспечения:

- дата (день, месяц, год) и время (часы, минуты, секунды) совершения работником действий с защищаемой информацией;

-присвоенный работнику идентификатор, позволяющий установить работника в автоматизированной системе, программном обеспечении;

-код, соответствующий технологическому участку*;

- результат совершения работником действия с защищаемой информацией (успешно или неуспешно);

- информация, используемая для идентификации устройств, при помощи которых либо в отношении которых осуществлен доступ к автоматизированной системе, программному обеспечению в целях совершения работником действий с защищаемой информацией.

*технологические участки:

ФПП	Формирование Агрегатором ЭС, передача и прием Агрегатором сформированных ЭС
ХИ	Хранение Агрегатором информации об осуществленных операциях по переводу денежных средств

VII. СКЗИ.

А) Обеспечение защиты информации при осуществлении переводов денежных средств с использованием СКЗИ осуществляется в соответствии с Федеральный закон N 63-ФЗ, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), и технической документацией на СКЗИ.

Б) Обеспечение защиты персональных данных с использованием СКЗИ осуществляется в соответствии с приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

В) В случае применения СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

VIII. При взаимодействии Банка и Агрегатора должно обеспечиваться подписание ЭС усиленной электронной подписью.

IX. Агрегатор должен обеспечить реализацию технологических мер по обеспечению защиты информации:

Требования к защите информации для БПА, осуществляющих операции платежного Агрегатора.

Операция	Защищаемая информация	Технологический участок	Действие	Технологические меры*						
				3	4	5	8	9	10	11
Формирование (подготовка) ЭС при обеспечении приема ЭСП Поставщиками услуг, при участии в переводе денежных средств в пользу Поставщиков услуг по операциям с использованием ЭСП	Информация, содержащаяся в: • ЭС при обеспечении приема ЭСП Агрегатором. • ЭС, направляемых Агрегатором Банку, ОУИО. • в реестрах ЭС при обеспечении приема ЭСП Агрегатором. Информация об осуществленных операциях по переводу денежных средств. Ключевая информация СКЗИ, используемая при осуществлении обмена ЭС между Агрегатором, Банком, ОУИО.	ФПП	Формирование Агрегатором ЭС, передача и прием Агрегатором сформированных ЭС	+	+	+	+	+		
		ХИ	Хранение Агрегатором информации об осуществленных операциях по переводу денежных средств						+	+

*Технологические меры:

3 - Применение механизмов и (или) протоколов формирования и обмена ЭС, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификацию входных ЭС.

4 - Взаимная (двухсторонняя) аутентификация Банка, Агрегатора, ОУИО.

5 - Использование простой или усиленной электронной подписи в соответствии с Федеральным законом N 63-ФЗ.

8 - Проверка соответствия (сверка) результатов осуществления операций, связанных с переводом денежных средств, с информацией, содержащейся в ЭС.

9 - Реализация мер, направленных на проверку правильности формирования (подготовки) ЭС (двойной контроль).

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.

11 - Восстановление защищаемой информации в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники.