RTM GROUP

Что нужно прибавить к 382, чтобы получить 719

RTM TECHNOLOGIES — первая экспертная компания, специализирующаяся на проведении нормативных и нормативно - технических экспертиз в области ИБ и ИТ.

rtmtech.ru

СОДЕРЖАНИЕ

Информация по срокам

- Основная часть положения вступает в силу с 1 января 2022 года
- Часть требований к ОПС в направлении эксплуатации СКЗИ вступает в силу с 1 января 2024 года, остальные требования для ОПС в направлении эксплуатации СКЗИ вступает в силу с 1 января 2031 года.
- С 1 января 2022 года 382-П признаётся утратившим силу.

Общие требования

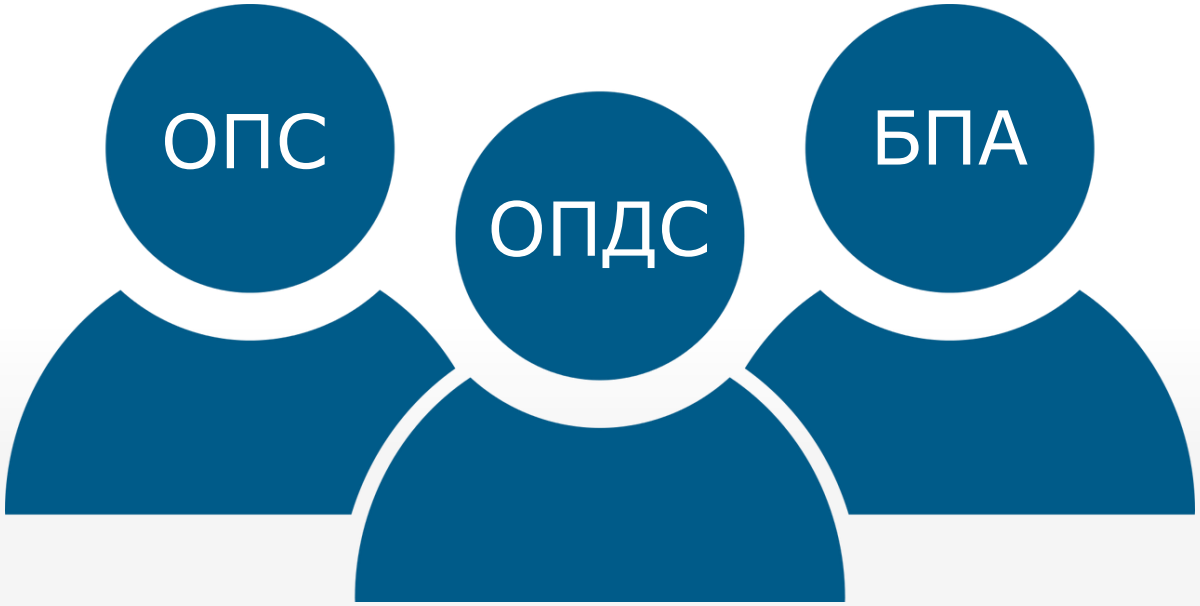
- Оценка по ГОСТ 57580 с привлечением сторонних организаций + требования по хранению отчета
- **Требование к оценке соответствия по ОУД 4**: данное требование присутствовало в 382-П, но не выполнялось, требование перешло в 719-П, и выполнять его **необходимо**.
- 719-П не распространяется на отношения, регулируемые Федеральным законом № 187-ФЗ

Субъекты регулирования 719-П

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

Банковский платёжный агент/субагент (БПА) - это ИП/юридические лица, оказывающие по условиям агентского договора банковские операции в сфере оборота денежных средств граждан в интересах кредитного учреждения.

Оператор платежной системы (ОПС) - юридическое лицо, определяющее правила платежной системы и выполняющее обязанности, предусмотренные законодательством



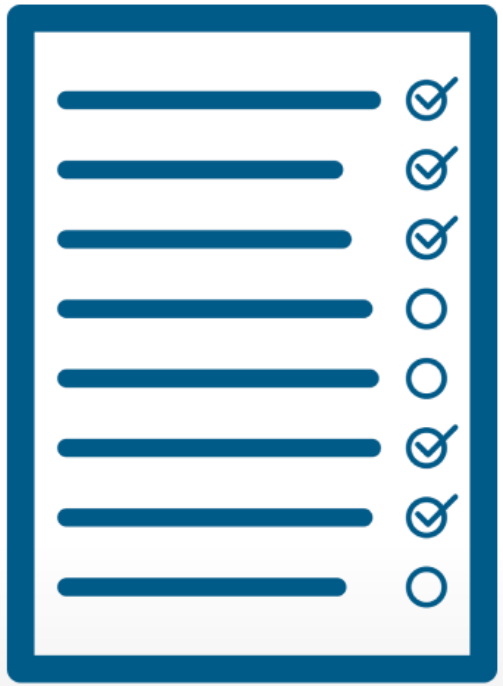
Теперь и они регулируются ЦБ

Оператор услуг информационного обмена (ОУИО) - организации, оказывающие российским кредитным организациям услуги обмена информацией при переводе средств с помощью электронных средств платежа между кредитной организацией и ее клиентами или между кредитной организацией и иностранным поставщиком платежных услуг.

Поставщик платежных приложений (ППП) – организации - разработчики, предоставляющие клиентам российских банков-партнеров программное обеспечение для осуществления переводов с помощью платежных карт.

Платежный агрегатор (ПА) — это платформа для приема денег на сайте. Она отвечает за перевод средств со счета покупателя на счет продавца. В основе сервиса лежит платежный шлюз.

Требования к операторам по переводу денежных средств



- Требования соответствия 683-П (соответствие ГОСТ 57580 не ниже 4 уровня / оценка проводится минимум раз в 2 года)
- Для системно значимых ОПДС – выполнение требований 131 приказа ФСТЭК, а именно сертификация прикладного программного обеспечения по 4 уровню доверия (для системно значимых ОПДС) и по 5 уровню доверия (для иных ОПДС)
- Требования к проведению контрольных мероприятий БПА в направлении информационной безопасности

Требования к банковским платёжным агентам/субагентам

- Выделение платежного агрегатора из БПА
- Возможность самостоятельного повышения уровня защиты информации на основе анализа рисков
- За исключением платежного агрегатора, БПА должны проводить тестирование на проникновение и анализ уязвимостей информационной безопасности
- Соответствие ГОСТ 57580:
  - ❖ реализация минимального уровня защиты информации для БПА
  - ❖ реализация не ниже 4 уровня соответствия, аудит проводится минимум раз в 2 года, для платёжных агрегаторов

Требования к операторам услуг информационного обмена

Требования к реализации стандартного уровня защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017 (соответствие не ниже 4 уровня / аудит проводится минимум раз в 2 года).

Требования к операторам платежной системы

- Требования к системе управления рисками
- Требования к системе управления инцидентами ИБ
- Требования к применению СКЗИ

Операторы значимой платежной системы должны обеспечить использование иностранных и отечественных СКЗИ, прошедших сертификацию с 1 января 2031 года.

Требования к операторам услуг платежной инфраструктуры

- Требования к защите информации при информационном обмене (обмене электронными сообщениями)
- Требования к ОУПИ, оказывающие услуги платежной инфраструктуры в рамках системно значимых платежных систем, должны реализовывать усиленный уровень защиты информации, а все остальные – стандартный по ГОСТ 57580 (аудит не реже раза в два года)
- Проведение оценки по ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013
- Требования к сертификации прикладного программного обеспечения по 4/5 уровню доверия в соответствии с приказом ФСТЭК России № 131.

Анализ технологических мер по обеспечению защиты информации

Для банковских платежных агентов/субагентов, операторов услуг информационного обмена, операторов услуг платежной инфраструктуры в приложении 1 к 719-П приведён перечень из **11 технологических мер защиты информации**.

Данное приложение отражает требования к **механизмам, модулям, протоколам безопасности**, применяемым в информационных системах, задействованных в переводе денежных средств.

Стоит отметить, что Организация, соответствующая 382-П, частично выполняет требования технологических мер защиты информации. Далее будут представлены новые требования, которым необходимо соответствовать субъектам регулирования.

Группировка требований технологических мер

1. Обеспечение хранения и возможность восстановления защищаемой информации

2. Реализация функции сверки результатов осуществления финансовых операций, реализация двойного контроля правильности формирования электронных сообщений

3. Реализация применения системы управления логическим доступом клиентов, сотрудников, участников обмена электронными сообщениями

63

4. Соблюдение законодательства в направлении использования электронной подписи.

Описание групп требований технологических мер

1.Обеспечение хранения и возможность восстановления защищаемой информации:

- 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;

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

2. Реализация функции сверки результатов осуществления финансовых операций, реализация двойного контроля правильности формирования электронных сообщений:

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

- Реализация мер, направленных на проверку правильности формирования (подготовки) электронных сообщений (двойной контроль).

Описание групп требований технологических мер

3.Реализация применения системы управления логическим доступом клиентов, сотрудников, участников обмена электронными сообщениями (идентификация, аутентификация, авторизация):

- Реализация механизма идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств.

- Реализация механизма двухфакторной аутентификации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств.

4. Соблюдение законодательства в направлении использования электронной подписи «перекочевали» из 382-П

Стоит отметить, что Организация, соответствующая 382-П, частично выполняет требования технологических мер защиты информации. Далее будут представлены новые требования, которым необходимо соответствовать субъектам регулирования.

Виды субъекты регулирования 719-П в направлении технологических мер

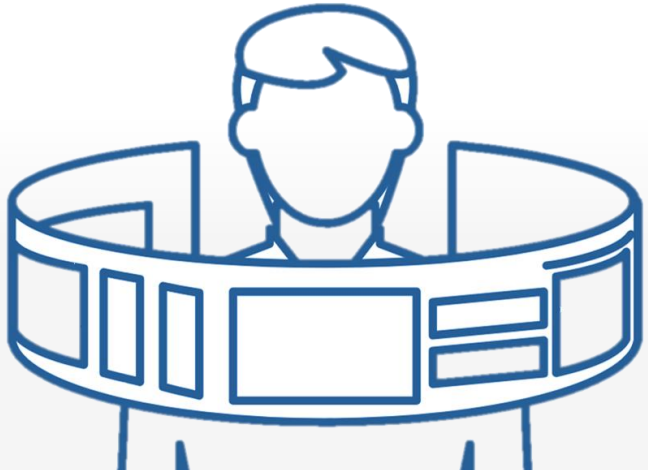
В приложении 2 к 719-П приведен перечень из 6 субъектов, которые обязаны выполнять технологические меры:

- Банковские платежные агенты (субагенты)
- Банковские платежные агенты, осуществляющие операции платежного агрегатора
- Операторы услуг информационного обмена
- Операторы услуг платежной инфраструктуры, осуществляющие деятельность операционных центров
- Операторы услуг платежной инфраструктуры, осуществляющие деятельность платежных клиринговых центров
- Операторы услуг платежной инфраструктуры, осуществляющие деятельность расчетных центров

Регулируемые субъекты обязаны реализовать данные технологические меры, применяемые для защиты информации, на следующих технологических участках:

- Формирование (подготовка), передача и прием электронных сообщений
- Хранение электронных сообщений и информации об осуществленных переводах денежных средств
- Идентификация, аутентификация и авторизация клиентов операторов по переводу денежных средств при совершении действий в целях осуществления операций по переводу денежных средств
- Удостоверение права клиентов операторов по переводу денежных средств распоряжаться денежными средствами
- Осуществление операций по переводу денежных средств, учет результатов их осуществления

Необходимо подчеркнуть, что требования применения технологических мер различаются в зависимости от вида субъекта регулирования, типа защищаемой информации, анализируемого технологического участка, а также осуществляемых операций.



СПАСИБО ЗА ВНИМАНИЕ!

Фёдор Музалевский

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group

+79081472741

f.muzalevsky@rtmtech.ru

https://rtmtech.ru

GroupRTM

rtm.group

@GroupRtm

rtm.group.Russia

t.me/kurilka_ib