RTM GROUP

Что делать некредитным финансовым организациям по информационной безопасности в 2022 году

rtmtech.ru

СОДЕРЖАНИЕ

Краткий обзор положения № 757-П

Положение № 757-П является основным элементом регулирования информационной безопасности и процессов защиты информации в некредитных финансовых организациях (НФО) со стороны Центрального банка (ЦБ).

Обязательные к исполнению требования по защите информации определены в Положении 757-П.

Оценка соответствия ОУД4 проводится в отношении программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети "Интернет".

Общие обязательные требования для **всех НФО**

Общие требования для НФО, имеющих один из трех уровней защиты информации

Минимальный | **Стандартный** | **Усиленный**

Требование о проведении оценки соответствия по ГОСТ 57580

Выполнение общих требований 757-П

Все без исключения некредитные финансовые организации должны были уже выполнить пункты:

Актуальные общие требования Положения 757-П и что они означают	
п.1.2 **п.1.3**	О защите информации с помощью **СКЗИ** в соответствии с 63-ФЗ, 152-ФЗ (защита **персональных данных**), Постановлением Правительства № 1119, Приказом ФСБ № 66 (ПКЗ-2005), Приказом ФСБ № 378
п.1.4.1	Ежегодное определение уровня защиты информации не позднее десятого рабочего дня календарного года.
п.1.8	Фиксация решения о применимости оценки соответствия **ОУД 4** в отношении :
	• ПО, распространяемого среди клиентов • ПО информационных систем, которые обрабатывают защищаемую информацию (в соответствии с п.1.1 Положения 757-П) • иное ПО – самостоятельно определяется необходимость соответствия требованиям ОУД 4

В ГОСТ Р 57580 есть три уровня защиты информации
В Положении 757-П для некоторых некредитиных финансовых организаций отсутствует требование соответствовать какому-либо из уровней ГОСТ
В таком случае Национальный Стандарт признается не применимым по отношению к некредитной финансовой организации

Краткий обзор федерального закона № 152-ФЗ

Федеральный закон N 152-ФЗ "О персональных данных«

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Аудит проводится на соответствие требованиям законодательства.

Краткий обзор ГОСТ 57580 дата введения 2018-01-01

Национальный стандарт российской федерации. безопасность финансовых (банковских) операций защита информации финансовых организаций базовый состав организационных и технических мер.

Требования ГОСТ, соответствующие усиленному, стандартному и минимальному уровню должны выполнять НФО в соответствии с п. 1.4.2., 1.4.3., 1.4.4.

Оценка соответствия уровня защиты информации некредитными финансовыми организациями, реализующими **усиленный уровень** защиты информации, должна осуществляться **не реже одного раза в год**, некредитными финансовыми организациями, реализующими **стандартный уровень** защиты информации, - **не реже одного раза в три года.**

Тестирование на проникновение и анализ уязвимостей (пентест)

Проводить тестирование на проникновение НФО реализующим усиленный и стандартный уровень необходимо в соответствии с п. 1.4.5

Пентест необходимо проводить ежегодно.

Краткий обзор оценка соответствия ПО (ОУД 4)

Проведение оценки соответствия по ОУД 4 в 757-П п.1.8. (стандартный и усиленный уровень)

Оценка проводится при каждой смене версии ПО.

Разбор сроков исполнения

Согласно 757-П:

Проведение оценки соответствия для усиленного **не реже одного раза в год**, с привлечением лицензиатов ФСТЭК (п.1.5.1).
Проведение оценки соответствия для стандартного **не реже одного раза в три года**, с привлечением лицензиатов ФСТЭК (п.1.5.1).
п. 1.7 вступает в силу с 01.01.2022 и действует по 30.07.2023 включительно.

С 1 января 2022

- Не ниже третьего
- Числовая оценка > 0,7

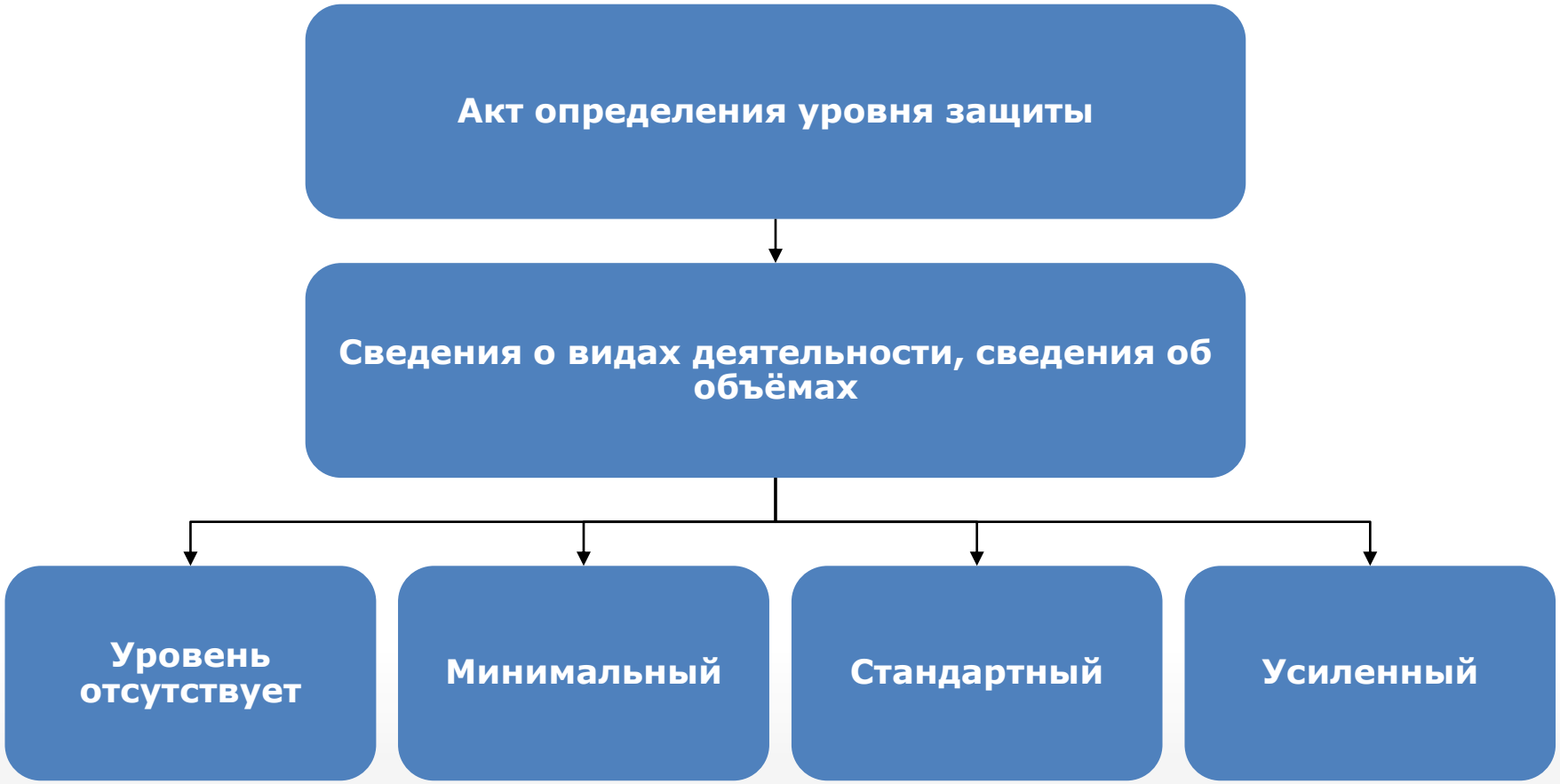
Разбор сроков исполнения

Согласно 757-П:

П. 1.4.4 Требования ГОСТ Р 57580.1-2017, соответствующие **минимальному** уровню защиты информации, должны соблюдать некредитные финансовые организации к 01.07.2022.

К 1 июля 2022

Обоснование неприменимости ГОСТ 57580



Сроки исполнения положений

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Музалевский Федор Александрович

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group

Кобец Дмитрий Андреевич

Эксперт в сфере информационной безопасности

Заместитель директора технического департамента RTM Group


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


GroupRTM


rtm.group


@GroupRtm


rtm.group.Russia


t.me/kurilka_ib