RTM GROUP

Разбор нового Положения ЦБ РФ № 757-П от 22 июня 2021 года

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

rtmtech.ru

Что нового?

Определять уровень защиты информации нужно не позднее **10 рабочего дня в году**

Регистраторы финансовых транзакций должны соответствовать **Усиленному** уровню по ГОСТ Р 57580 (с 1 января 2022 года)

Расширился перечень НФО, соответствующих **Стандартному** уровню по ГОСТ Р 57580

Добавились требования для НФО по соответствию **Минимального** уровня по ГОСТ Р 57580

Анализ уязвимостей по ОУД4 **заменен** на **оценку** соответствия по ОУД4

Добавились некоторые **общие требования** по обработке защищаемой информации

Сроки и требования к проведению оценки по ГОСТ 57580 **не поменялись**.
Отсутствует необходимость проведения оценки для **Минимального уровня**.

Кто соответствует Стандартному уровню по ГОСТ 57580 ?

Изменения:

- Специализированные депозитарии ИФ, ПИФ и НПФ, **размер активов которых превышает 1 трлн. рублей**
- Репозитарии, **не являющиеся регистраторами финансовых транзакций**
- Брокеры, дилеры, управляющие, депозитарии и регистраторы, **для которых определены условия, указанные в Положении 481-П**
- **Остальных НФО, «пришедших» из 684-П, изменения не коснулись**

Новый перечень НФО:

- **Оператор инвестиционной платформы** (во 2-4 квартал обслужили более 100 000 лиц)
- **Оператор финансовой платформы** (во 2-4 квартал обслужили более 100 000 лиц)
- **Оператор информационных систем**, которые выпускают ЦФА (во 2-4 квартал обслужили более 25 000 лиц)
- **Оператор обмена ЦФА** (во 2-4 квартал обслужили более 25 000 лиц)

Для «**нового**» перечня НФО в Главах 2 и 3 определены дополнительные требования
Главы 2 и 3 **вступают в силу** с 1 января 2022 года

Кто соответствует Минимальному уровню по ГОСТ 57580 ?

- **Специализированные депозитарии ИФ, ПИФ** и **НПФ**, стоимость активов которых менее 1 трл рублей
- **Брокеры, дилеры, управляющие, депозитарии** и **регистраторы**, не попадающие под условия соответствия Стандартному уровню
- **Управляющие компании ИФ, паевых ИФ** и **НПФ**;
- **Форекс-дилеры**;
- **Операторы финансовой платформы**, которым не нужно соответствовать Стандартному уровню
- **Операторы информационных систем**, **выпускающих ЦФА**, которым не нужно соответствовать Стандартному уровню
- **Оператор обмена ЦФА**, которым не нужно соответствовать Стандартному уровню
- **Страховые организации**, не попадающие под условия соответствия Стандартному уровню
- Общества **взаимного страхования**
- **Страховые брокеры**

Требования вступают в силу **с 1 июля 2022 года**
При **Минимальном** уровне **оценку** по ГОСТ Р 57580 **проводить не нужно**

Оценка соответствия по требованиям ОУД4

Анализ уязвимостей по ОУД4
заменен
на оценку соответствия по ОУД4

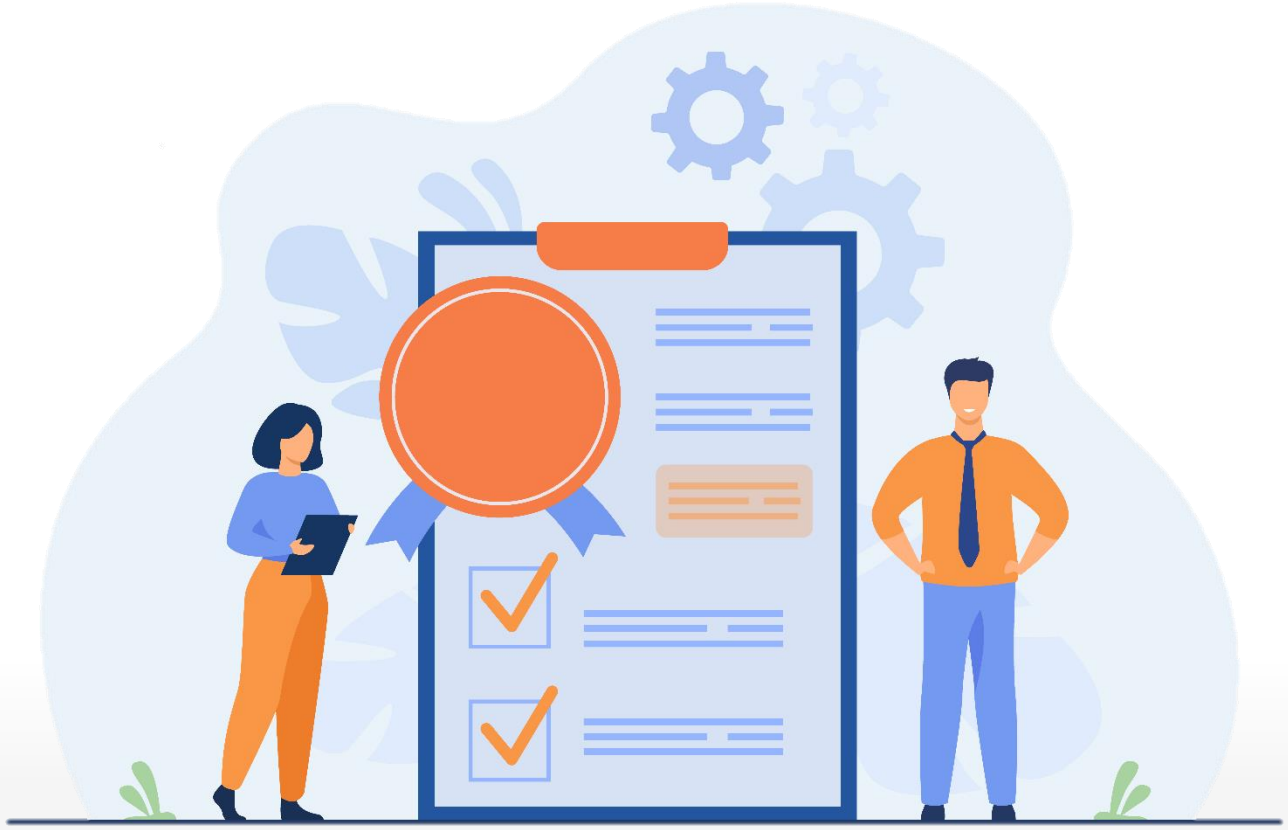
Оценку соответствия по ОУД4
можно делать самостоятельно
либо
с привлечением лицензиата ФСТЭК

Соответствие / Анализ уязвимостей

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Руководства	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Оценка задания по безопасности	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_VAN	1	2	2	3	4	5	5

Сертификация ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Сертификация на отсутствие НДВ
заменена
на сертификацию ФСТЭК
по 76 приказу



Сертификация ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для Усиленного уровня	Для Стандартного уровня
Сертификация по 4 уровню доверия	Сертификация по 5 уровню доверия

Решение о сертификации принимается самостоятельно.

Об изменениях среди общих требований

Большинство требований осталось без изменений.

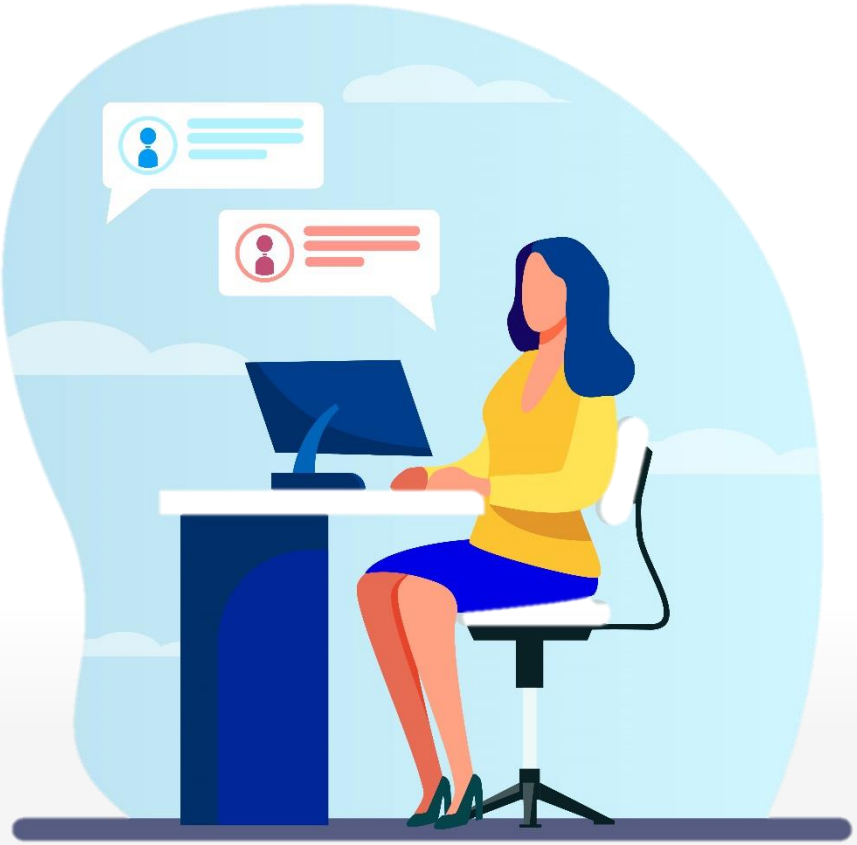
- НФО, реализующие **любой из уровней защиты**, должны выполнять требования по обработке информации об инцидентах ИБ
- НФО, реализующие **любой из уровней защиты**, должны доводить рекомендации до клиентов (ранее распространялось на **все НФО**)

Для тех, кто соответствует Стандартному и Усиленному уровням, необходимо:

- При проведении пентестов, осуществлять **устранение** выявленных **уязвимостей**
- **Применять УКЭП** или **УЭП** при подписании электронных сообщений, когда не выделен целевой сегмент в сети (если не используются выделенные каналы связи)
- При использовании **ЕИС** ПДн соответствовать требования **Приказа ФСТЭК № 21**
- При использовании **ЕСИА** соответствовать требованиям **Приказа Минкомсвязи № 210**
- Проводить **оценку** соответствия по требованиям к **ОУД.4**

Информирование ЦБ

1. Порядок информирования ЦБ РФ о сведениях об инцидентах ИБ должен быть регламентирован
2. Информация о принятых мерах и мероприятиях по реагированию на инциденты ИБ передается в ЦБ РФ
3. Информирование об используемых сайтах, необходимых для осуществления финансовой деятельности



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


8 800 201-20-70


info@rtmtech.ru


https://rtmtech.ru


GroupRTM


rtm.group


@GroupRtm


rtm.group.Russia


t.me/kurilka_ib