RTM GROUP

Выполнение общих требований Положения ЦБ РФ 757-П

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.

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

Какая информация подлежит защите?

В п.1.1. Положения определен перечень информации, в отношении которой распространяются требования по защите:

- Электронные документы, формируемые при осуществлении финансовых операций
- Криптографические ключи
- Информация, необходимая для авторизации клиентов
- Информация о проведенных финансовых операциях
- Персональные данные

Кто соответствует Усиленному уровню по ГОСТ 57580 ?

Перечень НФО:

- Центральные контрагенты
- Центральный депозитарий
- Регистраторы финансовых транзакций

Для Регистраторов финансовых транзакций Главе 2 определены дополнительные требования Главы 2 **вступают в силу** с 1 января 2022 года

Кто соответствует Стандартному уровню по ГОСТ 57580 ?

Перечень НФО:

- Специализированные депозитарии ИФ, ПИФ и НПФ, **размер активов которых превышает 1 трлн. Рублей**
- Страховые организации, стоимость активов превышает 20 миллиардов рублей за 6 календарных месяцев.
- Репозитарии, **не являющиеся регистраторами финансовых транзакций**
- Брокеры, дилеры, управляющие, депозитарии и регистраторы, **для которых определены условия, указанные в Положении 481-П**
- **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)
- Организаторы торговли

Для данного 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**

Выполнение общих требований

Все без исключения некредитные финансовые организации должны выполнять 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

Выполнение общих требований для НФО соответствующих усиленному и стандартному уровню защиты информации

Дополнительные пункты, для усиленного и стандартного уровня защиты информации:

Актуальные общие требования Положения 757-П и что они означают	
п.1.4.2	Осуществлять защиту информации в соответствии с требованиями ГОСТ 57580.1-2017 по усиленному/стандартному уровню ЗИ
п.1.4.5	Ежегодное тестирование объектов информационной инфраструктуры на предмет проникновения и анализ уязвимостей.
1.5	Обеспечения проведения оценки соответствия определенного ими уровня. Привлечение сторонних организаций лицензиатов ФСТЭК. Оценка соответствия **не реже одного раза в год** для усиленного уровня, **не реже одного раза в три года** для стандартного уровня
1.6	Требование по хранению отчета составленного проверяющей по результатам оценки соответствия ГОСТ 57580
1.7	Обеспечение уровня соответствия не ниже третьего (с 01.01.2022) и не ниже четвертого (01.07.2023)
1.8	Использование прикладного ПО, прошедших сертификацию ФСТЭК или оценку соответствия не ниже чем ОУД4.
1.9	Обеспечение целостности электронных сообщений
1.10	Требование по технологии безопасной обработке защищаемой информации
1.11	Требование по регистрации результатов выполнения действий, связанных с осуществлением доступа к ЗИ.
1.12	О хранении защищаемой информации, и обеспечении целостности и доступности ее.
1.13	Доведение рекомендаций до клиентов по защите от воздействия вредоносного кода, связанные с ним возможные риски
1.14	Требование по регистрации инцидентов защиты информации
1.15	Требование по информированию ЦБ.

Выполнение общих требований для НФО соответствующих минимальному уровню защиты информации

Дополнительные пункты, для минимального уровня защиты информации:

Актуальные общие требования Положения 757-П и что они означают	
п.1.4.4	Осуществлять защиту информации в соответствии с требованиями ГОСТ 57580.1-2017 по минимальному уровню ЗИ.
1.8	Самостоятельное определение необходимость сертификации или оценки соответствия не ниже чем ОУД 4 прикладного ПО
1.13	Доведение рекомендаций до клиентов по защите от воздействия вредоносного кода, связанные с ним возможные риски
1.14	Требование по регистрации инцидентов защиты информации
1.15	Требование по информированию ЦБ.

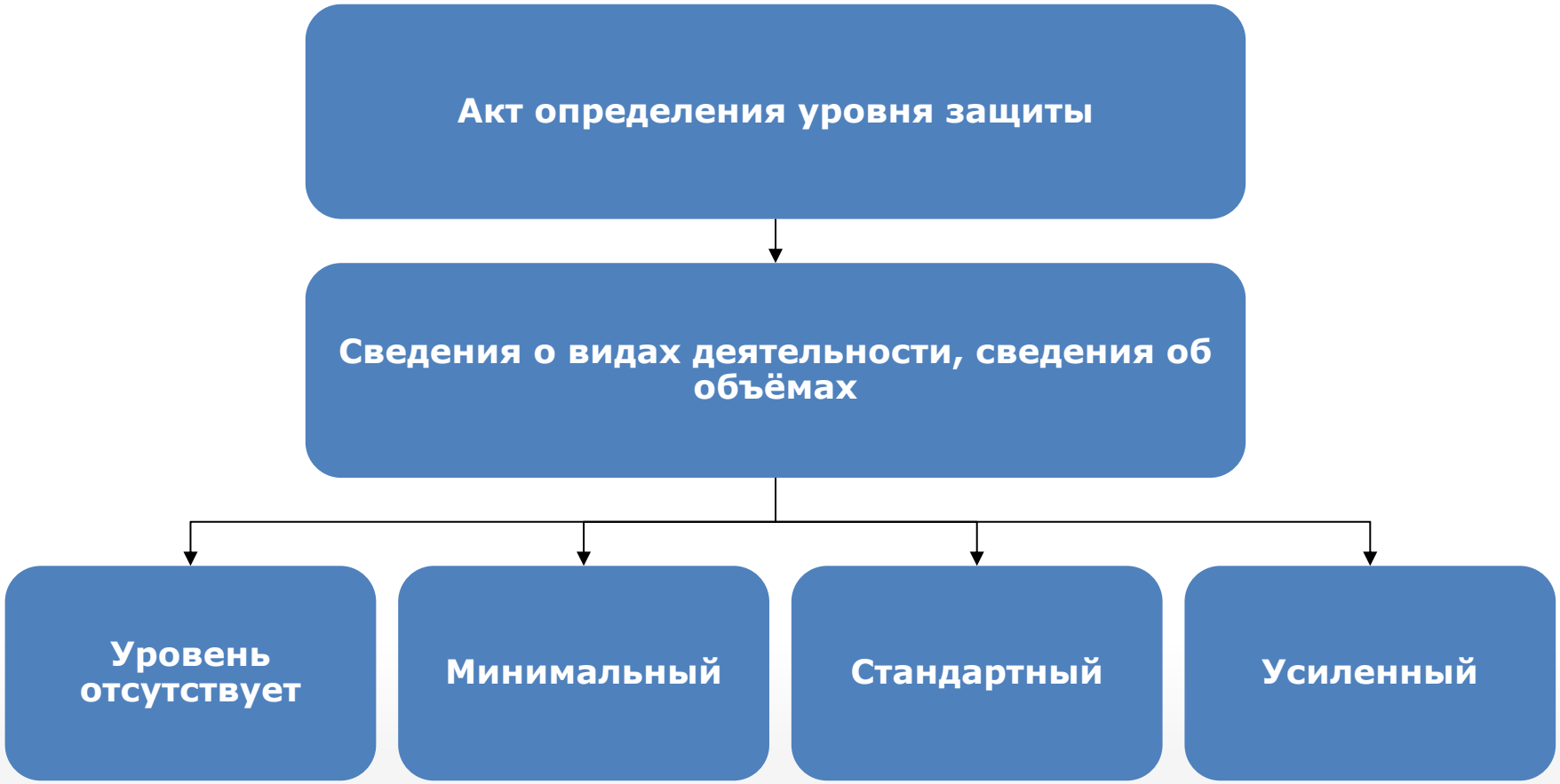
Защита персональных данных в рамках положения 757-П

Некредитным финансовым организациям необходимо проверить соответствие указанным нормативно-правовым актам (п.1.2 и п 1.3)

Персональные данные	СКЗИ
Постановление правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	**Приказ ФСБ № 66** «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»
Федеральный закон № 152-ФЗ «О персональных данных»	**Федеральный закон № 63-ФЗ** «Об электронной подписи»
Приказ ФСБ № 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 РФ требований к защите персональных данных для каждого из уровней защищенности»	

ВАЖНО!!!: в п.1.1 указано, что если в числе защищаемой информации содержатся персональные данные, то НФО должны соответствовать требованиям 19 статьи 152-ФЗ «О персональных данных»

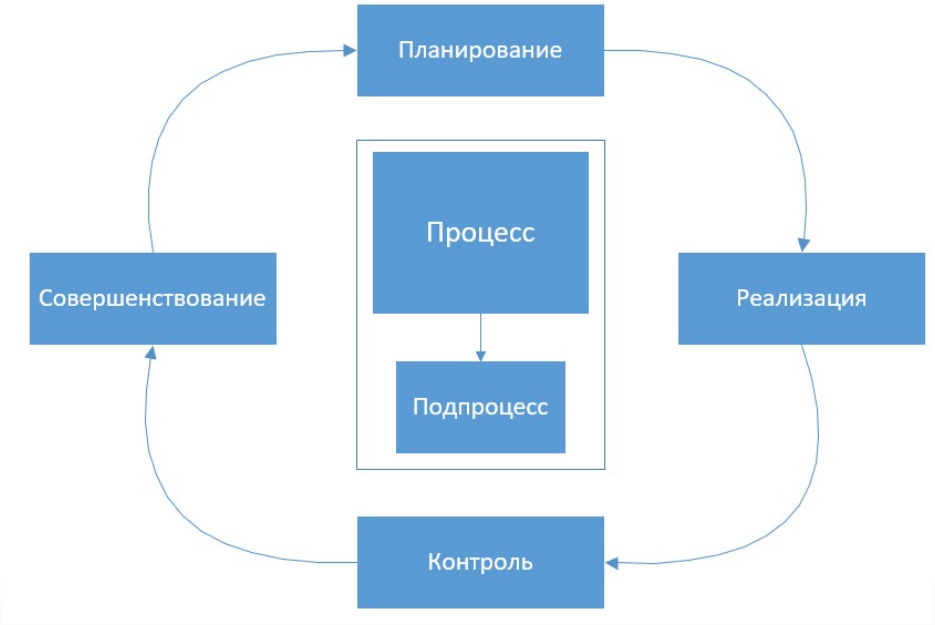
Обоснование неприменимости ГОСТ 57580



ГОСТ 57580

Процессы:

1. Обеспечение защиты информации при управлении доступом;
2. Обеспечение защиты вычислительных сетей;
3. Контроль целостности и защищенности информационной инфраструктуры;
4. Защита от вредоносного кода;
5. Предотвращение утечек информации;
6. Управление инцидентами защиты информации;
7. Защита среды виртуализации;
8. Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств



Направления защиты информации

Планирование	Реализация	Контроль	Совершенствование
1. Определить область применения процесса ЗИ	1. Должное применение мер ЗИ	1. Контроль области применения процесса ЗИ	1. Пересмотр применяемых мер ЗИ
2. Описать состав, содержание и порядок применения мер ЗИ	2. Назначение ответственных	2. Контроль знаний работников	2. Фиксация решений о необходимости совершенствования
	3. Применение ТСЗИ	3. Контроль должного применения мер ЗИ	

Меры ГОСТ Р 57580.1-2017

- Большинство организационных мер защиты информации реализуются за счет введения организационно-распорядительной документации
- Технические меры защиты информации реализуются за счет технических решений применяемых в информационной инфраструктуре Организации

Соотношение мер для 2-го уровня защиты

Применяемые технические решения для выполнения мер ГОСТ 57580

Процесс 1 «Обеспечение защиты информации при управлении доступом»

- Технологии разграничения доступа реализуемые операционной системой (Active Directory, Парольная политика и т.д.);
- Технологии разграничения доступа реализуемые сторонними средствами (СЗИ от НСДи т.д.);
- Средства регистрации событий в системах управления доступом;
- Системы управления физическим доступом (Физические замки, СКУД, Пожарная сигнализация и т.д.).

Процесс 2 «Обеспечение защиты вычислительных сетей»

- Межсетевые экраны;
- Криптошлюзы;
- IDS/IPS-системы;
- Антивирусы реализующие функции контроля отсутствия (выявления) аномальной сетевой активности;
- Функциональное оборудование беспроводного доступа

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

- Сканеры уязвимостей;
- Средства доверенной загрузки ПО
- Штатные средства аудита Windows

Процесс 4 «Защита от вредоносного кода»

- Антивирусное программное обеспечение;
- Многовендорный подход при реализации системы антивирусной защиты.

Применяемые технические решения для выполнения мер ГОСТ 57580

Процесс 5 «Предотвращение утечек информации»

- DLP-системы, которые должны включать следующие функции:
- Средства доверенного уничтожения информации.

Процесс 6 «Управление инцидентами защиты информации»

- SIEM/ITSM-системы.

Процесс 7 «Защита среды виртуализации»

- Функциональные средства виртуализации

Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

- MDM-системы;
- Технологии защищенной связи переносных устройств;
- Использование антивирусов на переносных устройствах.

Влияние технических решений на итоговую оценку по ГОСТ 57580

Сокращение базового набора мер

— За счет грамотной разработки модели угроз

Применение компенсирующих мер

— За счет грамотной разработки модели угроз и документов верхнего уровня (положения, политики)

Выполнение организационных мер

— За счет прямого документирования базовых либо компенсирующих мер

Меры	Н	О	Т
Базовый состав	98	290	279
Адаптированный состав	250	200	217
После компенсации	250	250	167

Влияние ОРД и технических решений на итоговую оценку по ГОСТ 57580

До разработки ОРД/После разработки ОРД

Наименование процесса системы ЗИ, направления ЗИ	Выбор	Планирование (0.2)	Реализация (0.4)	Контроль (0.25)	Совершенствование (0.15)	Оценка процесса
Процесс 1 «Обеспечение ЗИ при управлении доступом»	0,64	0,40/1,00	0,60	0,64/1,00	0,00/1,00	0,56/0,74
Процесс 2 «Обеспечение защиты сетей»	0,66	0,40/1,00	0,67	0,60/1,00	0,00/1,00	0,58/0,76
Процесс 3 «Контроль целостности и защищенности»	0,65	0,00/1,00	0,64	0,58/1,00	0,00/1,00	0,53/0,75
Процесс 4 «Защита от ВВК»	0,94	1,00/1,00	0,80	0,68/1,00	0,00/1,00	0,82/0,93
Процесс 5 «Предотвращение утечек»	0,25	0,00/1,00	0,22	0,09/1,00	0,00/1,00	0,18/0,47
Процесс 6 «Управление инцидентами»	0,56	0,20/1,00	0,67	0,38/1,00	0,88/1,00	0,43/0,71
Процесс 7 «Защита среды виртуализации»	0,65	0,00/1,00	0,64	0,58/1,00	0,00/1,00	0,53/0,75
Процесс 8 «Защита мобильных (переносных) устройств»	0,00	0,00	0,00	0,00	0,00	Н
Применение организационных и технических мер ЗИ на этапах жизненного цикла АС						0,37/0,67
Количество нарушений ЗИ, выявленных в результате оценки соответствия ЗИ						3
Итоговая оценка соответствия ЗИ						0,49/0,71

Разработкой ОРД можно достичь только третий уровень соответствия.
Исходя из положений ГОСТ уровень соответствия оценивается за каждый из процессов
Письмо ЦБ № 56-1-11/265 от 22.05.2020 г.

Как выполнить требования по ОУД4

1. Применяемое прикладное ПО для осуществления финансовых операций должно соответствовать требованиям ОУД4 **только** в НФО, которые реализуют **стандартный и усиленный уровни защиты информации** по ГОСТ 57580 (п.1.8)

2. Согласно абзацам 2 и 3 п.1.8 Положения 757-П некредитные финансовые организации, не реализующие стандартный и усиленный уровни (т.е. минимальный, отсутствие уровня) защиты информации **вправе самостоятельно принимать решение** о соответствии ПО требованиям ОУД.4

Обеспечивать соответствие не обязательно

В случае упомянутого выше **решения**, оценка соответствия прикладного ПО проводится **своими силами** или **с привлечением сторонней** организации (абзацы 3-4 п.1.8)

Примечание: Вместо оценки соответствия ПО требованиям ОУД.4 можно применять ПО, прошедшее сертификацию ФСТЭК. Для организаций не реализующих уровни отсутствуют требования соответствия уровням доверия (приказ ФСТЭК № 76)

Последствия невыполнения требований 757-П

Центральный Банк РФ является регулятором в сфере деятельности НФО

Регулятором в сфере защиты персональных данных является **Роскомнадзор**

Административная и уголовная ответственность

Штрафы и санкции со стороны регуляторов

Возможны **хищения приводящие к потерям как денежных средств, так и других ценностей** из-за невыполнения основных требований

Возможны **утечки информации**, в том числе персональных данных клиентов

Почему RTM-Group? Обзор наших услуг

- **Помощь в обосновании** неприменимости ГОСТ Р 57580**.** Формирование регламента для дальнейшего использования (ежегодного обоснования)
- **Проверка выполнения требований и организация** защиты персональных данных и применения СКЗИ
- **Помощь в принятии решения** о проведении оценки соответствия по требованиям ОУД.4
- **Разработка рекомендаций** для полного соответствия требованиям Положения 757-П

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