RTM GROUP

Внедрение основных метрик по операционной надежности – практический эффект

Вебинар для некредитных финансовых организаций

RTM GROUP

Эксперты вебинара

Кобец Дмитрий

Заместитель директора технического департамента

Чекудаев Кирилл

Ведущий консультант по управлению рисками

Окорокова Валерия

Младший консультант по информационной безопасности

RTM GROUP

О чем пойдет речь

01 Требования регулятора

02 Описание и цели операционной надежности

03 Формальный и неформальный подход к ОН

04 Метрики операционной надежности

05 Заполнение форм отчетности по 779-П

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Работаем на всей территории России, Беларуси и Казахстана, и не ограничиваемся на этом. Головной офис компании находится в Москве, производственное подразделение базируется в Воронеже.

RTM Group ежегодно выполняет сотни проектов, делая свой вклад в стабильность и безопасность киберпространства, а также помогает провести анализ цифровых доказательств для судов и следственных органов.

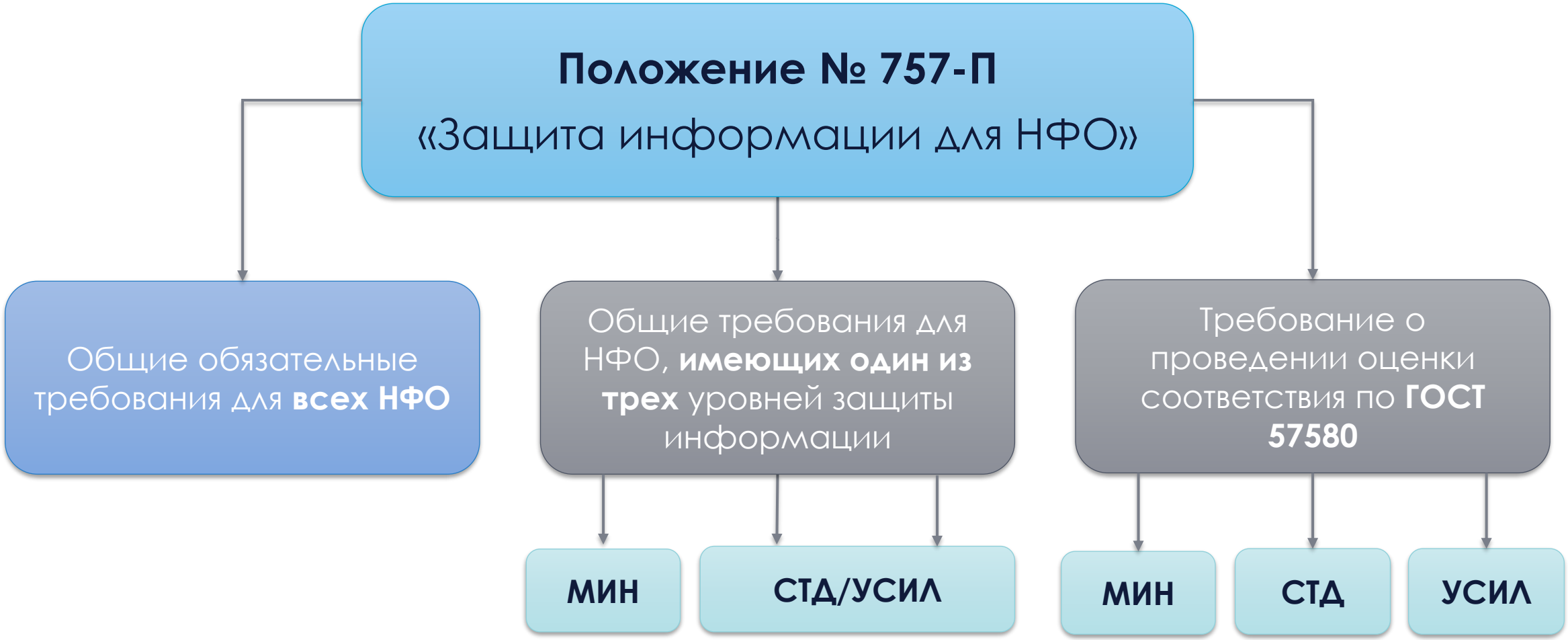
1700+ Экспертиз проведено нашими экспертами

700+ Аудитов проведено по различным критериям

50+ Вариантов аудитов ИБ в нашем портфеле

45+ Вариантов производимых экспертиз

01. Требования регулятора


Положение № 757-П
«Защита информации для НФО»
Общие обязательные требования для всех НФО
Общие требования для НФО, имеющих один из трех уровней защиты информации
Требование о проведении оценки соответствия по ГОСТ 57580
МИН
СТД/УСИЛ
МИН
СТД
УСИЛ

Общие обязательные требования для **всех НФО**

п.1.2, п.1.3

Защита информации с помощью СКЗИ

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 ОУД4

В 757-П НФО могут быть без уровня. ГОСТ 57580 – не применим

757-П

С 1 июля 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка по ГОСТ 57580:
- Усиленный (1 уровень) раз в год
- стандартный (2 уровень) раз в 3 года

Привлечение лицензиатов ФСТЭК (п.1.5.1).

02. Описание и цели операционной надежности

Что такое операционная надежность

Операционная надежность (ОН) – это способность некредитной финансовой организации непрерывно реализовывать свои технологические процессы.

Главным нормативным документом, регулирующим область операционной надежности для НФО является Положение Банка России от 15 ноября 2021 г. №779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

Цели операционной надежности

- Непрерывность процесса
- Защищенность информационной инфраструктуры
- Соблюдение требований 779-П
- Определение и выполнение целевых показателей
- Оптимизация технологических и бизнес-процессов
- Взаимодействие элементов информационной инфраструктуры

В пределах обеспечения операционной надежности НФО должны:

- Обеспечить непревышение порогового уровня допустимого времени простоя технологического процесса
- Соблюдать требования к взаимодействию с поставщиками услуг в сфере IT
- Принимать технические и организационные меры
- Вести учет и контроль элементов критичной архитектуры и взаимодействий между ними
- Обеспечить нейтрализацию информационных угроз
- Информировать Банк России о выявленных событиях операционного риска, связанных с нарушением операционной надежности

RTM GROUP

03. Формальный и неформальный подход к ОН

3.1 Формальный подход

1. Определение и описание состава процедур
2. Планирование применения организационных и технических мер
3. Определение перечня и порядка организационного взаимодействия подразделений
4. Выделение ресурсного обеспечения для выполнения требований к операционной надежности
5. Моделирование информационных угроз в отношении критичной архитектуры

3.2 Формальный подход

6. Порядок утверждения и условия пересмотра процедур
7. Регистрация данных, превышающих целевые значения, причины и реагирование
8. Информирование ЦБ РФ о выявленных событиях риска операционной надежности и публичных мероприятиях
9. Определение порядка осуществления контроля соблюдения требований к операционной надежности в рамках системы внутреннего контроля
10. Обеспечение реализации требований к операционной надежности на стадиях создания, ввода в эксплуатацию, эксплуатации, модернизации, вывода из эксплуатации объектов информационной инфраструктуры

3.3 Практический подход

1. Установление жестких требований по обеспечению операционной надежности для поставщиков услуг в области ИС
2. Определение технологических участков технологических процессов и ответственности за их функционирование
3. Поиск потенциальных угроз операционной надежности
4. Обучение персонала и борьба с внутренними нарушителями
5. Установление целевых показателей ниже нормативных
6. Постоянное тестирование (контроль) системы операционной надежности

3.4 Применение практического подхода. Пример №1

Обучение персонала и борьба с внутренними нарушителями позволит:

- Повысить готовность персонала реагировать на внешние угрозы
- Снизить время реагирования на инциденты
- Сократить количество невыполненных операций в период инцидентов
- Снизить потери в оборотных средствах, операционной прибыли, а также репутационные риски
- Снизить доли деградации технологических процессов

3.5 Применение практического подхода. Пример №1

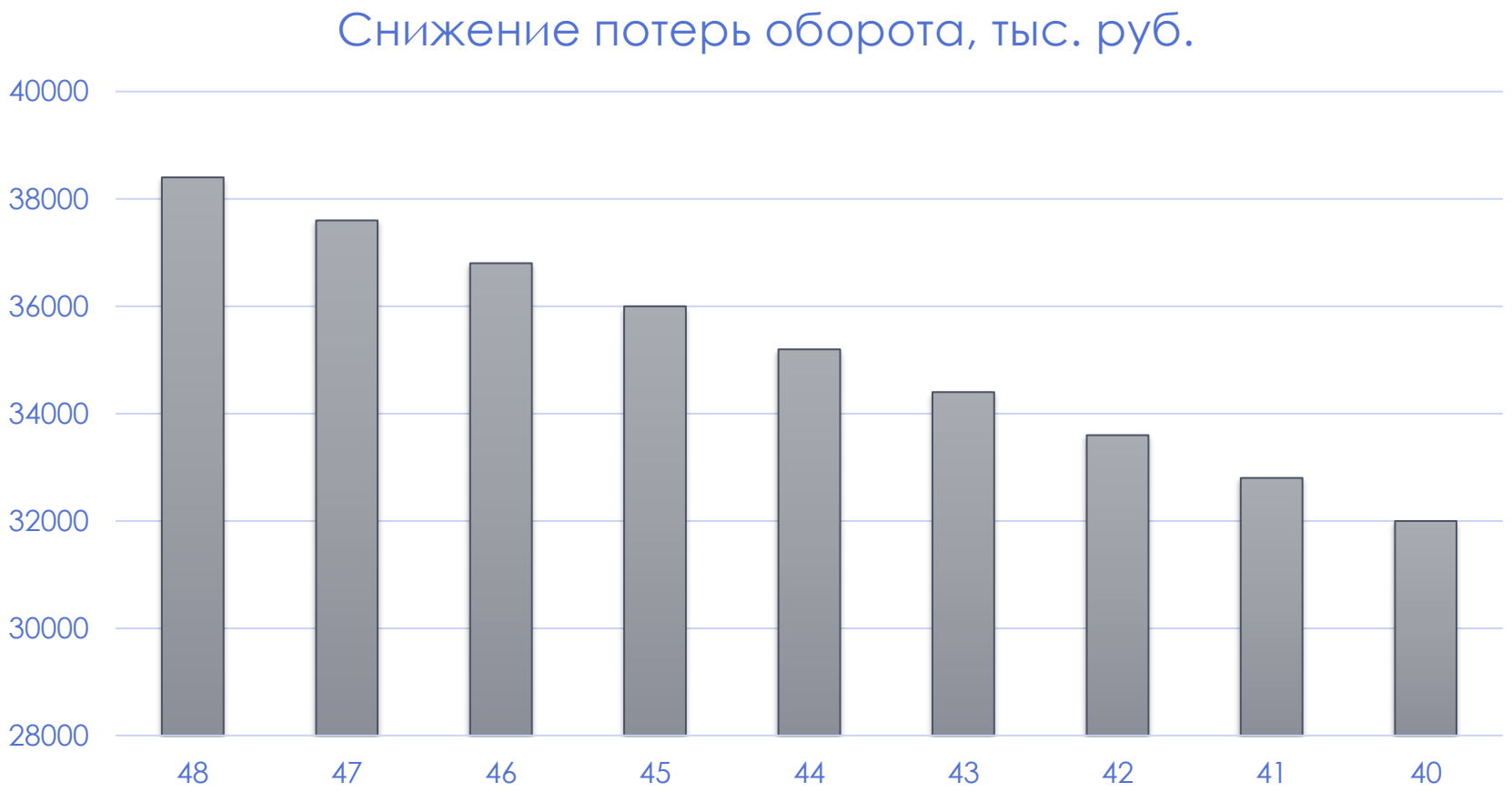
	Формальный подход	Практический подход	Изменение
Количество операций в период деградации	6800	6000	-800
Общее количество операций непрерывного функционирования	480688	481488	800
Доля деградации процесса, %	1,414639	1,246137	-0,1685

3.6 Применение практического подхода. Пример №2

Установление жестких требований по обеспечению операционной надежности поставщиков услуг в области ИС позволит:

- Обязать поставщиков услуг в области ИС разработать политику и план обеспечения операционной надежности
- Снизить время реагирования на инциденты операционной надежности у поставщиков услуг
- Обеспечить надежность предоставляемых поставщиками услуг
- Снизить зависимость ИС НФО от инцидентов у поставщиков услуг
- Снизить потери оборотных средств и прибыли

3.7 Применение практического подхода. Пример №2



RTM GROUP

04. Метрики операционной надежности

4. Метрики операционной надежности

Целевой показатель	Определение
Допустимая доля деградации технологического процесса	Общее количество операций в период событий операционного риска, связанных с нарушением операционной надежности / общее количество операций непрерывного функционирования
Допустимое время простоя и (или) деградации технологических процессов кредитных организаций в рамках инцидента операционной надежности	Не превышающие значения, установленных приложением 1 Положения 779-П
Допустимое суммарное время простоя и (или) деградации технологического процесса кредитной организации	Общее допустимое время простоя в случае превышения допустимой доли деградации технологического процесса в течение очередного календарного года
Показатель соблюдения функционирования технологического процесса	Время начала, окончания, продолжительности и последовательности процедур в рамках технологического процесса

Определяются для каждого технологического процесса

4.1 Пример расчета метрик операционной надежности

№	Код технологического процесса	Наименование технологического процесса	Допустимое время простоя и (или) деградации технологического процесса, в минутах	Допустимая доля деградации технологического процесса	Допустимое суммарное время простоя и (или) деградации технологического процесса, в минутах	Продолжительность времени работы (функционирования) технологического процесса, в часах			
						I квартал	II квартал	III квартал	IV квартал
1	2	3	4	5	6	7	8	9	10
1	ТПрКО1	Технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами	240	0,006834	1215	684	732	780	768
2	ТПрКО2	Технологический процесс, обеспечивающий осуществление регистратором сверки учитываемых регистратором прав на ценные бумаги с центральным депозитарием по счету номинального держателя центрального депозитария	240	0,007879	1401	684	732	780	768
3	ТПрКО3	Технологический процесс, обеспечивающий возможность совершения участниками финансовой платформы финансовых сделок с использованием финансовой платформы	240	0,004683	833	684	732	780	768

05. Заполнение форм отчетности по 779-П

Наименование показателя	Описание технологического процесса	Продолжительность времени работы (функционирования) технологического процесса
	1	2
Код технологического процесса		
[ТПрНФО1]	Технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами	432

Наименование показателя	Допустимое время простоя и (или) деградации технологического процесса	Допустимая доля деградации технологического процесса	Допустимое суммарное время простоя и (или) деградации технологического процесса	Суммарное время простоя и (или) деградации технологического процесса
	1	2	3	4
Код технологического процесса				
[ТПрНФО1]	2	0,07	24	24

Наименование показателя	Полное фирменное наименование оператора связи	Идентификацион-ный номер налогоплательщика (ИНН)	TIN
	1	2	3
Идентификатор оператора связи			
	ООО "Оператор связи"	1454564	214654

Наименование показателя			IP-адрес или пул IP-адресов в формате протокола IPv4	IP-адрес или пул IP-адресов в формате протокола IPv6	Номер авто-номной системы
			1	2	3
Код технологичес-кого процесса	**Код технологичес-кого участка**	**Наименование объекта информатизации**			
[ТПрНФО1]	**ИАА**	**АРМ "ИС НПФ"**	172.16.105.32	2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d	AS 64511

Наименование показателя	Номера телефонов, используемые отчитывающейся организацией для взаимодействия с клиентами
	1
2023-06-30	7900-900-900

Наименование показателя		IP-адрес или пул IP-адресов в формате протокола IPv4	IP-адрес или пул IP-адресов в формате протокола IPv6
		1	2
Доменное имя электронного адреса информационного ресурса	Унифицированный идентификатор информационного ресурса (URI-адрес)		
NFO.com	https://NFO.sootvetstvie.ru	192.168.0.1.	1050:0:0:0:5:600:300c:326b

Наименование показателя		Информация об автоматизированных системах и приложениях
		1
Код технологического процесса	Код технологического участка	
[ТПрНФО1]	ИАА	ИС "Первая"
[ТПрНФО1]	ФПП	ИС "Вторая"

Наименование показателя			Код функциональности (возможностей), получаемой (получаемых) отчитывающейся организацией в рамках облачных решений, предоставляемых поставщиком услуг	Код категории облачных решений, предоставляемых поставщиком услуг	Адрес (место нахождения) центра обработки данных, предоставляющего услуги отчитывающейся организации	Идентификационный номер налогоплательщика (ИНН)	TIN	Сведения о наличии у центра обработки данных сертификации	Информация о наличии соглашения, определяющего требования, предъявляемые к уровню качества предоставляемых сервисов (SLA), между отчитывающейся организацией и оператором центра обработки данных	Параметры надежности и отказоустойчивости, согласованные между отчитывающейся организацией и оператором центра обработки данных	Информация об автоматизированных системах и приложениях
			1	2	3	4	5	6	7	8	9
Код технологического процесса	Код технологического участка	Полное фирменное наименование оператора центра обработки данных									
[ТПрНФО1]	ИАА	ООО "Облако"	ФИИ	ИИИ	Москва, ул. Московская, д.1	0000000001	-	TIER III	Нет	-	ИС "Первая"

Наименование показателя	Тип документа (выпадающий список)	Тип документа (если выбрано Иное)	Наименование файла	Комментарий
	1	2	3	4
Идентификатор строки				

Информация о документах, включенных в состав пакета с отчетностью

Наименование показателя	2023-06-30				
	Фамилия, имя, отчество (последнее - при наличии) лица, ответствен-ного за предметную область отчетности (исполнителя)	Должность лица, ответственного за предметную область отчетности (исполнителя)	Номер телефона лица, ответствен-ного за предметную область отчетности (исполнителя)	Признак нулевого отчета	Наименование ИТ-разработчика, реализующего формирование отчетности в формате XBRL
ОКУД-0420401					
ОКУД-0420402					
ОКУД-0420404					
ОКУД-0420406					

Сопроводительная информация к отчетности.
Сведения об ответственных лицах за предметные области

Наименование показателя	Код территории по ОКАТО	Идентифи-кационный номер налого-плательщика (ИНН)	Основной государственный регистрационный номер (ОГРН) или основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП)	Полное фирмен-ное наиме-нование	Сокращенное фирменное наименование (при наличии)	Почтовый адрес отчитываю-щейся организации	Фамилия, имя, отчество (последнее – при наличии), подписавшего отчетность	Должность лица, подписавшего отчетность	Основание исполнения обязанностей лица, подписавшего отчетность	Показатели деятельности
2023-06-30										

Сопроводительная информация об отчитывающейся организации

RTM GROUP

Спасибо за внимание!

Ведущая консалтинговая компания
в области информационной
безопасности, судебной
экспертизы и ИТ-права.

+7 (495) 197-64-95

info@rtmtech.ru

rtm.group

https://rtmtech.ru