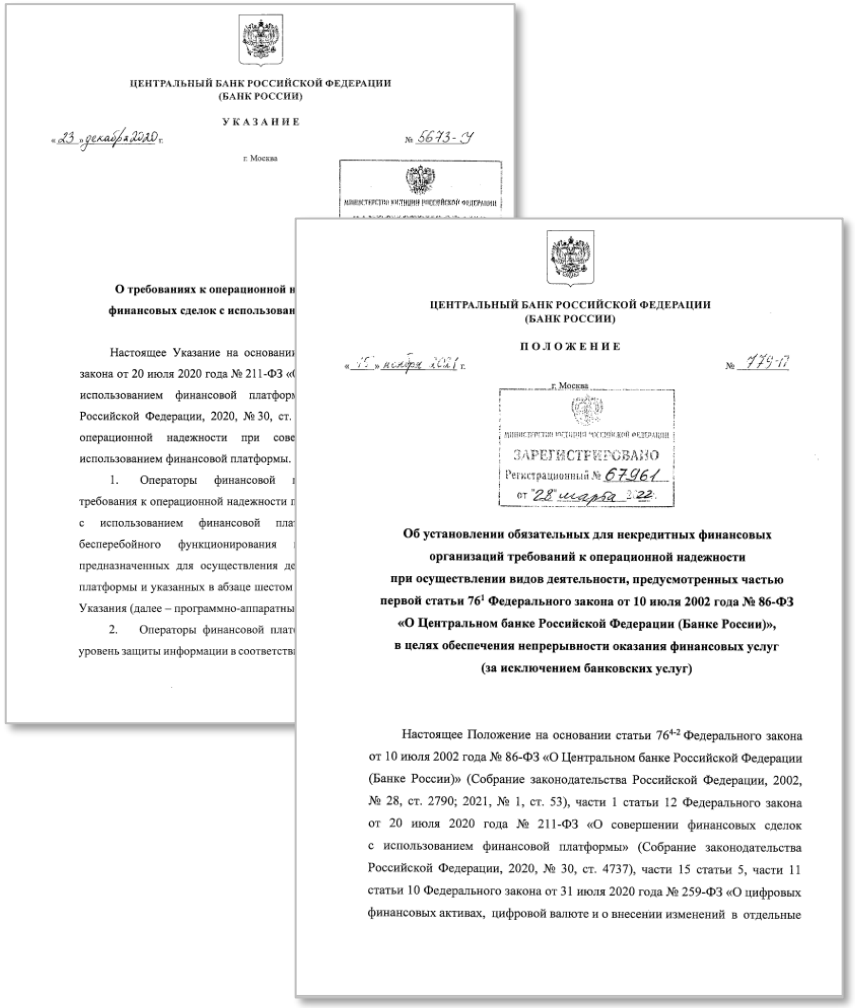
MOEX GROUP

MOEX.COM

ПРАКТИЧЕСКИЕ ВОПРОСЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПОЛОЖЕНИЯ № 779-П

ПОДГОТОВЛЕНО: Демидов С.В.
ДИРЕКТОР ДЕПАРТАМЕНТА ОПЕРАЦИОННЫХ РИСКОВ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НЕПРЕРЫВНОСТИ БИЗНЕСА

О КАКИХ ТРЕБОВАНИЯХ ИДЕТ РЕЧЬ?



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

«23» декабря 2020 г. № 5673-У

г. Москва

О требованиях к операционной н
финансовых сделок с использован

Настоящее Указание на основани
закона от 20 июля 2020 года № 211-ФЗ «
использованием финансовой платфор
Российской Федерации, 2020, № 30, ст.
операционной надежности при сове
использованием финансовой платформы.

1. Операторы финансовой
требования к операционной надежности
с использованием финансовой пла
бесперебойного функционирования
предназначенных для осуществления де
платформы и указанных в абзаце шестом
Указания (далее – программно-аппаратны

2. Операторы финансовой плат
уровень защиты информации в соответстви

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«15» ноября 2021 г. № 779-П

г. Москва

ЗАРЕГИСТРИРОВАНО
Регистрационный № 67961
от "28" марта 2022

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)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)

Настоящее Положение на основании статьи 76[4-2] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 1, ст. 53), части 1 статьи 12 Федерального закона от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (Собрание законодательства Российской Федерации, 2020, № 30, ст. 4737), части 15 статьи 5, части 11 статьи 10 Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные

- 23.12.2020 утверждено Указание Банка России № 5673-У «О требованиях к операционной надежности при совершении финансовых сделок с использованием финансовой платформы», вступление в силу для ОФП с 01.10.2021;
- 15.11.2021 утверждено Положение Банка России № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 761 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)» - вступление в силу с 01.10.2022. Отчетность в ЦБ с 01.04.2022. Первый отчет за 1Q 2022 – 01.07.2022

ПОЛОЖЕНИЕ БАНКА РОССИИ №779-П

ЧТО УСТАНАВЛИВАЕТ

Обязательные для некредитных финансовых организаций требования к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)

НА КОГО РАСПРОСТРАНЯЕТСЯ

Некредитные финансовые организации, осуществляющие виды деятельности, предусмотренные частью первой статьи 76.1 Федерального закона № 86-ФЗ

ВСТУПЛЕНИЕ В СИЛУ:

01.10.2022

Для НФО, обязанных соблюдать минимальный уровень – 01.01.2023

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ОПЕРАЦИОННАЯ НАДЕЖНОСТЬ

Способность обеспечить непрерывность функционирования критически важных процессов с учетом соблюдения целевых показателей операционной надежности.

ДЕГРАДАЦИЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Нарушение технологических процессов, приводящего к неоказанию или ненадлежащему оказанию финансовых услуг по причине **реализации информационных угроз.**

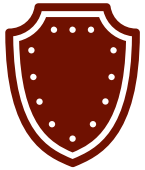
ИНФОРМАЦИОННЫЕ УГРОЗЫ

Источник реализации события риска информационной безопасности (в результате компьютерной атаки).

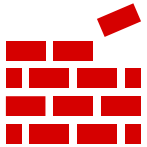
ОСНОВНЫЕ ПОЛОЖЕНИЯ

Основные требования Положения Банка России № 779-П

Требования к установлению целевых показателей операционной надежности



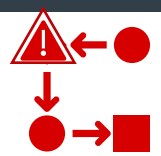
Требования к обеспечению операционной надежности



Требования к организации обеспечения операционной надежности

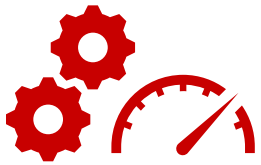
Требования к информированию Банка России о событиях операционного риска, связанных с нарушением операционной надежности

ПОКАЗАТЕЛИ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ



Допустимая доля деградации технологических процессов

отношение общего количества финансовых сделок, заключенных во время деградации технологических процессов к ожидаемому количеству финансовых сделок за тот же период в случае бесперебойного функционирования



Показатель соблюдения режима работы (функционирования) технологического процесса

отношение суммарного времени деградации сервисов к общему времени функционирования Платформы за вычетом суммарного времени технологических окон

от 2 до 24 часов

Допустимое время простоя и (или) деградации технологических процессов

отношение фактической продолжительности времени штатного функционирования Платформы к нормативной

Допустимое суммарное время простоя и (или) деградации технологических процессов

суммарное время простоя и (или) деградации технологических процессов Платформы за отчетный календарный месяц

ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

1. Учет и контроль состава элементов критичной архитектуры
2. Управление изменениями критичной архитектуры
3. Выявление, регистрация событий операционного риска, связанных с нарушением операционной надежности, и реагирование на них, а также восстановление
4. Взаимодействие с поставщиками услуг в сфере информационных технологий
5. Сценарный анализ (в части возможной реализации информационных угроз) и тестирование готовности противостоять реализации информационных угроз в отношении критичной архитектуры
6. Управление риском реализации информационных угроз со стороны внутреннего нарушителя
7. Обеспечение осведомленности некредитной финансовой организации об актуальных информационных угрозах
8. Управление риском возникновения зависимости обеспечения операционной надежности от ключевых работников
9. Защита критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы работников
10. Противодействие целевым компьютерным атакам в зависимости от уровня опасности

ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

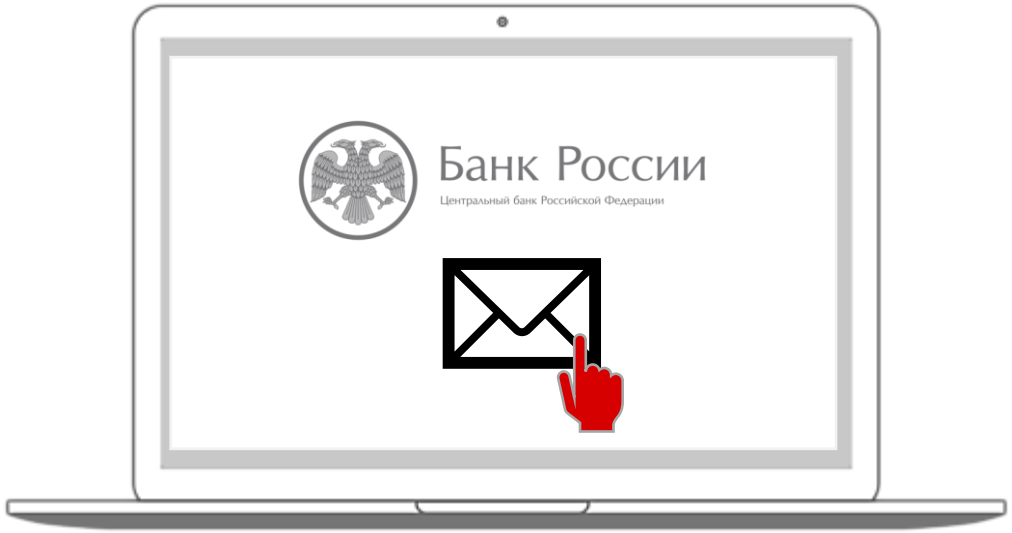
Установление во внутренних документах

- Определения и описания состава процедур в рамках обеспечения операционной надежности
- Определение организационной структуры некредитной финансовой организации, задействованной в обеспечении операционной надежности (с учетом исключения конфликта интересов), в том числе в части внутреннего контроля (при наличии)
- Выделение ресурсного обеспечения
- Порядка утверждения и условия пересмотра процедур в рамках обеспечения операционной надежности

В целях обеспечения операционной надежности некредитные организации должны

- Моделировать информационные угрозы в отношении критичной архитектуры
- Планировать применение организационных и технических мер, направленных на реализацию требований к операционной надежности, с учетом результатов оценки риска реализации информационных угроз в рамках системы управления рисками (при наличии)
- Обеспечивать реализацию требований к операционной надежности на этапах жизненного цикла объектов информационной инфраструктуры
- Обеспечивать контроль соблюдения требований к операционной надежности
- Определить порядок регистрации событий операционного риска, связанных с нарушением операционной надежности

ИНФОРМИРОВАНИЕ БАНКА РОССИИ



Использование в целях информирования технической инфраструктуры (автоматизированной системы) Банка России*
Или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры Банка России)

- О выявленных событиях операционного риска, связанных с нарушением операционной надежности (в случае превышения допустимой доли деградации технологических процессов)
- О принятых мерах и проведенных мероприятиях по реагированию на выявленное некредитной финансовой организацией или Банком России событие операционного риска, связанное с нарушением операционной надежности
- О планируемых мероприятиях по раскрытию информации, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на своих официальных сайтах в сети «Интернет»*

*не позднее одного рабочего дня до дня проведения мероприятия

ОБЩАЯ ИНФОРМАЦИЯ

Целевые показатели обеспечения операционной надежности определяются для следующих видов деятельности ПАО Московская Биржа:

- организатор торговли,
- оператор финансовой платформы,
- оператор обмена цифровых финансовых активов [1]

в целях обеспечения непрерывности оказания финансовых услуг в условиях **реализации информационных угроз**.

Операционная надежность – способность обеспечить непрерывность функционирования критически важных процессов с учетом соблюдения целевых показателей операционной надежности.

Деградация технологического процесса – нарушение технологических процессов, приводящего к неоказанию или ненадлежащему оказанию финансовых услуг по причине **реализации информационных угроз.**

Информационные угрозы – источник реализации события риска информационной безопасности (в результате компьютерной атаки).

[1] реализация требований к обеспечению операционной надежности при осуществлении деятельности оператора обмена цифровых финансовых активов будет осуществляться по факту запуска деятельности оператора обмена цифровых финансовых активов

ЦЕЛЕВЫЕ ПОКАЗАТЕЛИ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

1. ДОЛЯ ДЕГРАДАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

$$К_{Д} = \frac{D}{F}$$

D - общее количество финансовых операций, совершенных во время деградации технологического процесса в рамках СОР ОН, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг),
F - ожидаемое количество финансовых операций тот же период в случае непрерывного оказания финансовых услуг.

2. ДОПУСТИМОЕ ВРЕМЯ ПРОСТОЯ И (ИЛИ) ДЕГРАДАЦИИ (Д) технологического процесса в рамках СОР ОН (в случае превышения допустимой доли деградации технологического процесса), не выше порогового уровня.

3. ДОПУСТИМОЕ СУММАРНОЕ ВРЕМЯ ПРОСТОЯ И (ИЛИ) ДЕГРАДАЦИИ $Д_1$ технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу каждого календарного месяца.

$$Д_1 = \sum_{i=1}^{12} e_i$$

4. ПОКАЗАТЕЛЬ СОБЛЮДЕНИЯ РЕЖИМА РАБОТЫ (ФУНКЦИОНИРОВАНИЯ)

$$F = \frac{\sum DP}{(\sum H - \sum W)}$$

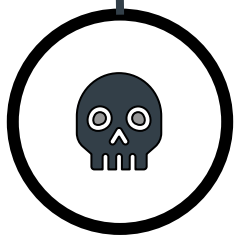
DP - время деградации технологических процессов, которые привели к нарушению оказания финансовых услуг.
H – общее время функционирования технологических процессов за отчетный период
W - временя проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов оказания финансовых услуг.

ПОРОГОВЫЕ ЗНАЧЕНИЯ ЦЕЛЕВЫХ ПОКАЗАТЕЛЕЙ ОБЕСПЕЧЕНИЯ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

	ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС	Допустимое время простоя и (или) деградации (Д0), ч [1]	Допустимое суммарное время простоя и (или) деградации (Д), ч [2]	Допустимая доля деградации (Кд) , % [3]	Показатель соблюдения режима работы (F), % [4]
ОРГАНИЗАТОР ТОРГОВЛИ	1. Технологический процесс, обеспечивающий заключение договора между участниками торгов	X	Y	Z	N
	2. Технологический процесс, обеспечивающий ведение реестра участников торгов и их клиентов, реестра заявок, реестра заключенных на организованных торгах договоров, реестра внебиржевых договоров	X	Y	Z	N
	3. Технологический процесс, обеспечивающий раскрытие и предоставление информации организатором торговли	X	Y	Z	N
ОПЕРАТОР ФИНАНСОВОЙ ПЛАТФОРМЫ	1. Технологический процесс, обеспечивающий возможность совершения участниками финансовой платформы финансовых сделок с использованием финансовой платформы	X	Y	Z	N
ОПЕРАТОР ОБМЕНА ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ	1. Технологический процесс, обеспечивающий возможность совершения сделок с цифровыми финансовыми активами	X	Y	Z	N
	2. Технологический процесс, обеспечивающий взаимодействие с оператором информационной системы	x	Y	Z	N

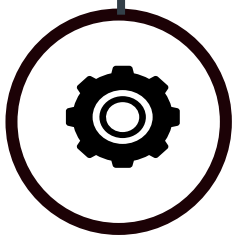
[1] Определяется регуляторно согласно 779-П
[2] Совпадает с допустимым временем простоя и (или) деградации для ОТ и ОО ЦФА
[3] Определяется как доступность для большинства участников торгов (более Z%)
[4] Определяется как пороговое значение показателей риск-аппетита «Доступность систем реального времени, %» и «Доступность систем, обеспечивающих прочие клиентские сервисы, %»

НАПРАВЛЕНИЯ РАЗВИТИЯ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ



Кибер безопасность

- организационные и технические меры, направленные на разработку сценарного анализа и проведение с использованием сценарного анализа тестирования готовности НФО противостоять реализации информационных угроз в отношении критичной архитектуры
- обеспечение осведомленности об актуальных информационных угрозах.



Контроль критичной архитектуры

- предотвращение возникновения уязвимостей в критичной архитектуре
- планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение бесперебойного функционирования программно-аппаратных средств;
- управление конфигурациями программно-аппаратных средств;
- управление уязвимостями и обновлениями программно-аппаратных средств.

Инцидент менеджмент

- выявление и регистрация инцидентов ОН,
- восстановление функционирования технологических процессов и программно-аппаратных средств после реализации инцидентов операционной надежности;
- анализ причин и последствий реализации инцидентов ОН;
- организацию взаимодействия между подразделениями НФО, а также между НФО и Банком России, иными участниками.

Вендор менеджмент

- управление риском реализации информационных угроз при привлечении поставщиков услуг, в том числе защиту программно-аппаратных средств от возможной реализации информационных угроз, включая компьютерные атаки, со стороны поставщиков услуг;
- управление риском технологической зависимости функционирования программно-аппаратных средств НФО от поставщиков услуг.

Риски и непрерывность

- Анализ рисков и угроз непрерывности бизнеса
- Выделение потенциально возможных сценариев ЧС, меры по снижению вероятности ЧС
- Меры по восстановлению критичных процессов при ЧС
- Поддержание резервных площадок и мощностей;
- Регулярные тестирования.