Банк России

РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОПЕРАЦИОННОЙ НАДЕЖНОСТИ НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Департамент информационной безопасности

2022 г.

Цели регулирования защиты информации и операционной надежности

1. Создание правовых условий для обеспечения защиты информации и операционной надежности

- отдельных финансовых организаций
- финансовых объединений
- финансовых экосистем (маркетплейс)

2. Сбалансированное регулирование

- риск-ориентированный подход
- обеспечение интересов потребителей (безопасные сервисы)

3. Прозрачность и унификация подходов по реализации требований за счет внедряемых стандартов

Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» — **Статья 76.4-1**

Положение Банка России от 20.04.2021 № 757-П

Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций

Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» — **Статья 76.4-2**

Положение Банка России от 15.11.2021 № 779-П

Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)

Правовые условия для обеспечения защиты информации и операционной надежности

реализация Банком России своих полномочий

исполнение требований закона участниками финансового рынка

Обеспечение защиты информации согласно установленным требованиям на уровнях

- инфраструктуры
- прикладного программного обеспечения
- технологий обработки данных

Обеспечение операционной надежности согласно установленным требованиям в отношении

- целевых показателей операционной надежности
- процедур обеспечения операционной надежности
- информирования об инцидентах

снижение хищений в общем объеме операций и поддержание непрерывности предоставления финансовых услуг

Подход к регулированию и надзору

Нормативное регулирование

Создание/обновление НПА

Переход к требованиям на трех уровнях:

- инфраструктуры (ГОСТ Р 57580.1);
- уровень ППО;
- технологии

Стандартизация

Разработка и сопровождение национальных и отраслевых стандартов

Технологии

Анализ деятельности организаций (учет специфики), разработка технологических мер

Банк России

РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

ПОЛОЖЕНИЕ БАНКА РОССИИ № 757-П

Основные подходы к установлению требований по защите информации

1 **Требования к защите информации в отношении объектов информационной инфраструктуры**

- реализация уровней защиты согласно ГОСТ Р 57580.1-2017
- ежегодное тестирование на проникновение и анализ уязвимостей
- независимая оценка соответствия уровням защиты информации согласно ГОСТ Р 57580.2-2018

2 **Требования к защите информации в отношении прикладного ПО АС и приложений**

- использование сертифицированных или прошедших оценку соответствия по требованиям к оценочному уровню доверия (ОУД) прикладного ПО АС и приложений

3 **Требования к защите информации в отношении технологии обработки защищаемой информации**

4 **Требования к информированию Банка России об инцидентах защиты информации**

5 **Требования в отношении применения СКЗИ**

6 **Требования в отношении применения электронной подписи**

Основные подходы к установлению требований по защите информации

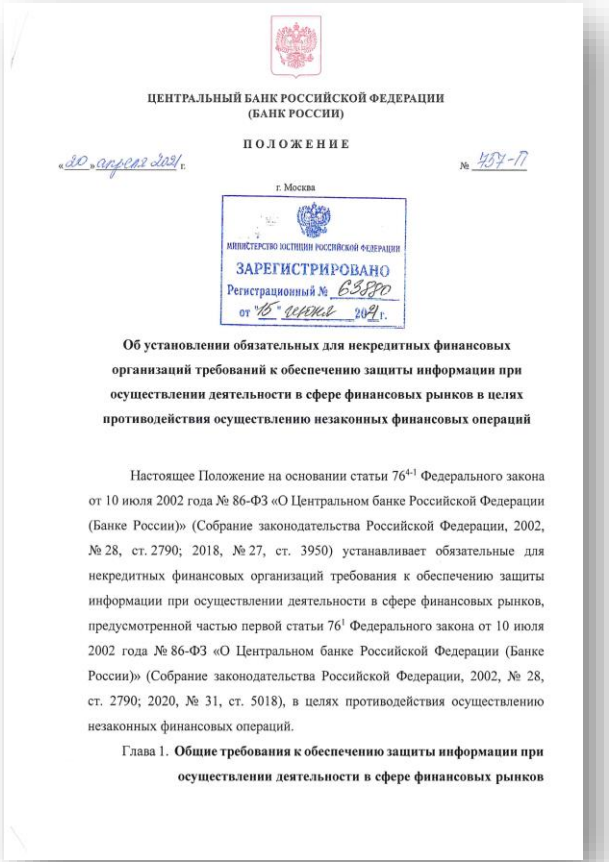
- управление учетными записями и правами субъектов логического доступа
- идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа
- защита информации при осуществлении физического доступа
- идентификация, классификация и учет ресурсов и объектов доступа

- сегментация и межсетевое экранирование вычислительных сетей
- выявление сетевых вторжений и атак
- защита информации, передаваемой по вычислительным сетям
- защита беспроводных сетей;

- мониторинг и анализ событий защиты информации
- обнаружение инцидентов защиты информации и реагирование на них

Положение Банка России № 757-П

Субъектный состав	Некредитные финансовые организации, осуществляющие виды деятельности, предусмотренные частью 1 статьи 76^{1} Федерального закона № 86-ФЗ	
Вступило в силу	03.07.2021	
Взамен	Положение Банка России от 17.04.2019 № 684-П	
Отложенные нормы	**01.07.2023**	Реализация стандартного и усиленного уровней защиты информации согласно ГОСТ Р 57580.1-2017 не ниже четвертого
	01.01.2024	Отдельное требование к технологии обработки защищаемой информации оператором информационной системы, в которой осуществляется выпуск ЦФА
Основание	статья 76^{4-1} Федерального закона № 86-ФЗ	



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«20» апреля 2021 г. № 757-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 63330
от 15 июня 2021 г.

Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций

Настоящее Положение на основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2018, № 27, ст. 3950) устанавливает обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью первой статьи 76^{1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2020, № 31, ст. 5018), в целях противодействия осуществлению незаконных финансовых операций.

Глава 1. **Общие требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков**

Основные изменения в рамках Положения Банка России № 757-П

1. **расширен субъектный состав, скорректирован подход к классификации некредитных финансовых организаций на организации крупных, средних и малых форм**

2. **установлены положения, регулирующие особенности обеспечения защиты информации отдельных НФО**

   - Операторы финансовых платформ (Глава 3)
   - Регистраторы финансовых транзакций (Глава 3)
   - Операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов (Глава 4)
   - Операторы обмена цифровых финансовых активов (Глава 4)

3. **уточнены показатели, которые определяют необходимость НФО соответствовать усиленному и стандартному уровням защиты информации, определенным в ГОСТ Р 57580.1**

4. **уточнены формулировки в части сертификации и оценки соответствия прикладного программного обеспечения для гармонизации с положением 719-П**

5. **введена новая категория некредитных финансовых организаций, реализующих минимальный уровень защиты информации**

6. **дополнены требования к порядку информированию**

Банк России

РЕГУЛИРОВАНИЕ В ОБЛАСТИ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

ПОЛОЖЕНИЕ БАНКА РОССИИ № 779-П

Основные требования Положения Банка России № 779-П

Основные положения

1

Требования к установлению целевых показателей операционной надежности

2

Требования к обеспечению операционной надежности

3

Требования к организации обеспечения операционной надежности

4

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

Особенности обеспечения операционной надежности для отдельных некредитных финансовых организаций	оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов	оператор обмена цифровых финансовых активов

Требования к установлению целевых показателей операционной надежности

1 **Обеспечить непревышение значения порогового уровня:**

- допустимого времени простоя технологических процессов
- допустимого времени деградации технологических процессов

2 **Определить во внутренних документах значений целевых показателей для каждого технологического процесса некредитных финансовых организаций**

- допустимое время простоя и (или) деградации технологических процессов в рамках события операционного риска, связанного с нарушением операционной надежности (в случае превышения допустимой доли деградации технологического процесса)*
- допустимая доля деградации технологического процесса
- допустимое суммарное время простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение двенадцати календарных месяцев к первому числу каждого календарного месяца
- показатель соблюдения режима работы (функционирования) технологического процесса (время начала, время окончания, продолжительность и последовательность процедур в рамках технологического процесса)

* Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов некредитных финансовых организаций приведены в Приложении к Положению Банка России № 779-П

3 **Обеспечить контроль за соблюдением значений целевых показателей операционной надежности**

4 **Не реже одного раза в год проводить анализ необходимости пересмотра значений целевых показателей операционной надежности**

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

1

Информирование 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

2

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

* информация размещается на официальном сайте Банка России в сети «Интернет»

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**

Учет и контроль состава элементов критичной архитектуры

Перечень элементов критичной архитектуры
Технологические процессы, реализуемые непосредственно некредитной финаносовой организацией
Подразделения (работники) некредитной финансовой организации, ответственные за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов
Объекты информационной инфраструктуры некредитной финансовой организации, задействованные при выполнении каждого технологического процесса
Технологические участки технологических процессов
Технологические процессы, технологические участки технологических процессов, реализуемые поставщиками услуг в сфере информационных технологий
Субъекты доступа, задействованные при выполнении каждого технологического процесса
Взаимосвязи и взаимозависимости некредитной финансовой организации с иными некредитными финансовыми организациями, кредитными организациями и поставщиками услуг в рамках выполнения технологических процессов
Каналы передачи защищаемой информации, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса

Требования к организации обеспечения операционной надежности

1

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

2

В целях обеспечения операционной надежности кредитные 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

Банк России

СПАСИБО ЗА ВНИМАНИЕ!