



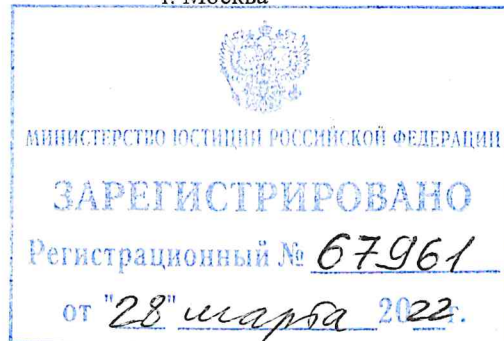
ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

« 15 » ноября 2021 г.

№ 779-17

г. Москва



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)

Настоящее Положение на основании статьи 76⁴⁻² 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

законодательные акты Российской Федерации» (Собрание законодательства Российской Федерации, 2020, № 31, ст. 5018) устанавливает обязательные для некредитных финансовых организаций требования 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)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2013, № 30, ст. 4084; 2021, № 27, ст. 5187), в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг).

Глава 1. Общие требования к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)

1.1. Некредитные финансовые организации должны обеспечивать операционную надежность при осуществлении ими видов деятельности, предусмотренных частью первой статьи 76¹ Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – деятельность в сфере финансовых рынков), с использованием автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее – объекты информационной инфраструктуры) путем обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг) (далее – финансовые услуги) в условиях реализации информационных угроз.

1.2. Некредитные финансовые организации, осуществляющие деятельность профессиональных участников рынка ценных бумаг, центрального депозитария, регистраторов финансовых транзакций,

управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда, специализированных депозитариев инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда, центрального контрагента, организатора торговли, субъектов страхового дела, негосударственных пенсионных фондов, операторов инвестиционных платформ, операторов финансовых платформ, операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторов обмена цифровых финансовых активов, клиринговую деятельность, репозитарную деятельность, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации в соответствии с подпунктами 1.4.2–1.4.4 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 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», зарегистрированного Министерством юстиции Российской Федерации 15 июня 2021 года № 63880 (далее соответственно – Положение Банка России от 20 апреля 2021 года № 757-П, некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации), в рамках обеспечения операционной надежности должны в соответствии с приложением к настоящему Положению обеспечить непревышение:

порогового уровня допустимого времени простоя технологических процессов, обеспечивающих осуществление деятельности в сфере финансовых рынков (далее – технологические процессы);

порогового уровня допустимого времени нарушения технологических процессов, приводящего к неоказанию или ненадлежащему оказанию финансовых услуг (далее – деградация технологических процессов).

1.3. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны определить во внутренних документах для каждого осуществляемого ими технологического процесса, указанного в приложении к настоящему Положению, значения следующих целевых показателей операционной надежности:

допустимого отношения общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг (далее – события операционного риска, связанные с нарушением операционной надежности), к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг (далее – доля деградации технологических процессов);

допустимого времени простоя и (или) деградации технологического процесса в рамках события операционного риска, связанного с нарушением операционной надежности (в случае превышения допустимой доли деградации технологического процесса), не выше порогового уровня, установленного в приложении к настоящему Положению;

допустимого суммарного времени простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу каждого календарного месяца;

показателя соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса).

Значение допустимой доли деградации технологических процессов должно рассчитываться некредитной финансовой организацией, обязанной соблюдать усиленный, стандартный или минимальный уровень защиты информации, на основании статистических данных за период не менее двенадцати календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности, за исключением случая, предусмотренного абзацем седьмым настоящего пункта, и (или) иных данных, обосновывающих их определение (по выбору некредитной финансовой организации).

В случае если технологический процесс функционирует менее двенадцати календарных месяцев, некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны определять значение допустимой доли деградации технологических процессов на основании статистических данных за период с даты начала его функционирования и (или) иных данных, обосновывающих их определение (по выбору некредитной финансовой организации).

В случае превышения допустимой доли деградации технологических процессов некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны обеспечить фиксацию:

фактического времени простоя и (или) деградации технологического процесса, исчисляемого по каждому событию операционного риска, связанному с нарушением операционной надежности (с момента нарушения технологического процесса по причине реализации события операционного риска, связанного с нарушением операционной надежности, до момента восстановления выполнения технологического процесса);

фактической доли деградации технологического процесса, исчисляемой по каждому событию операционного риска, связанному с нарушением

операционной надежности;

суммарного времени простоя и (или) деградации технологического процесса за последние двенадцать календарных месяцев, предшествующих событию операционного риска, связанному с нарушением операционной надежности.

При определении времени простоя и (или) деградации технологических процессов в расчет не включаются периоды времени проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны обеспечить контроль за соблюдением значений целевых показателей операционной надежности.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны не реже одного раза в год проводить анализ необходимости пересмотра значений целевых показателей операционной надежности, по итогам которого указанные некредитные финансовые организации должны пересмотреть значения целевых показателей операционной надежности либо принять мотивированное решение об отсутствии необходимости в пересмотре указанных значений.

В случае если законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций, обязанных соблюдать усиленный, стандартный или минимальный уровень защиты информации, установлена обязательность наличия у них системы управления рисками, указанные некредитные финансовые организации должны выполнять требования настоящего пункта в рамках системы управления рисками.

1.4. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны обеспечивать организацию учета и контроля следующих элементов (при их наличии) (далее при совместном упоминании – критичная архитектура):

технологических процессов, указанных в приложении к настоящему Положению, реализуемых непосредственно некредитной финансовой организацией;

подразделений (работников) некредитной финансовой организации, ответственных за разработку технологических процессов, указанных в приложении к настоящему Положению, поддержание их выполнения, их реализацию;

объектов информационной инфраструктуры некредитной финансовой организации, задействованных при выполнении каждого технологического процесса, указанного в приложении к настоящему Положению, реализуемого непосредственно некредитной финансовой организацией;

технологических участков предусмотренных приложением к настоящему Положению технологических процессов, указанных в пункте 1.10 Положения Банка России от 20 апреля 2021 года № 757-П (далее – технологические участки технологических процессов), реализуемых непосредственно некредитной финансовой организацией;

технологических процессов, указанных в приложении к настоящему Положению, технологических участков технологических процессов, реализуемых внешними контрагентами, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов (далее – поставщики услуг);

работников некредитной финансовой организации или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной

инфраструктуры некредитной финансовой организации (далее – субъекты доступа), задействованных при выполнении каждого технологического процесса, указанного в приложении к настоящему Положению;

взаимосвязей и взаимозависимостей между некредитной финансовой организацией и иными некредитными финансовыми организациями, кредитными организациями и поставщиками услуг в рамках выполнения технологических процессов, указанных в приложении к настоящему Положению (далее при совместном упоминании – участники технологического процесса);

каналов передачи защищаемой информации, указанной в пункте 1.1 Положения Банка России от 20 апреля 2021 года № 757-П, обрабатываемой и передаваемой в рамках технологических процессов, указанных в приложении к настоящему Положению, участниками технологического процесса.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в отношении своих элементов критичной архитектуры, являющихся значимыми объектами критической информационной инфраструктуры в соответствии с пунктом 3 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) (далее – Федеральный закон от 26 июля 2017 года № 187-ФЗ), должны выполнять требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 года № 187-ФЗ (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736).

В целях организации учета и контроля состава технологических процессов, указанных в приложении к настоящему Положению,

технологических участков технологических процессов, реализуемых поставщиками услуг, некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны обеспечивать ведение реестра указанных технологических процессов и технологических участков технологических процессов в соответствии со своими внутренними документами.

1.5. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны обеспечивать выполнение следующих требований в отношении управления изменениями критичной архитектуры:

управление уязвимостями в критичной архитектуре, с использованием которых могут реализоваться информационные угрозы и которые могут повлечь отклонение от значений целевых показателей операционной надежности, указанных в пункте 1.3 настоящего Положения;

планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение непрерывного оказания финансовых услуг;

управление конфигурациями объектов информационной инфраструктуры некредитных финансовых организаций;

управление уязвимостями и обновлениями (исправлениями) объектов информационной инфраструктуры некредитных финансовых организаций.

1.6. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны обеспечивать в отношении выявления, регистрации событий операционного риска, связанных с нарушением операционной надежности, и реагирования на них, а также восстановления выполнения технологических процессов, указанных в приложении к настоящему Положению, и функционирования своих объектов

информационной инфраструктуры после реализации указанных событий выполнение следующих требований:

выявление и регистрацию событий операционного риска, связанных с нарушением операционной надежности;

реагирование на события операционного риска, связанные с нарушением операционной надежности, в отношении критичной архитектуры;

восстановление выполнения технологических процессов, указанных в приложении к настоящему Положению, и функционирования своих объектов информационной инфраструктуры после реализации событий операционного риска, связанных с нарушением операционной надежности;

проведение анализа причин и последствий реализации событий операционного риска, связанных с нарушением операционной надежности;

организацию взаимодействия между подразделениями (работниками) некредитной финансовой организации, ответственными за разработку технологических процессов, указанных в приложении к настоящему Положению, поддержание их выполнения, их реализацию, между собой и Банком России, иными участниками технологического процесса в рамках реагирования на события операционного риска, связанные с нарушением операционной надежности, и восстановления выполнения технологических процессов, указанных в приложении к настоящему Положению, а также функционирования своих объектов информационной инфраструктуры после реализации событий операционного риска, связанных с нарушением операционной надежности.

1.7. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны обеспечивать выполнение следующих требований в отношении взаимодействия с поставщиками услуг:

управление риском реализации информационных угроз при привлечении поставщиков услуг, в том числе защиту своих объектов информационной инфраструктуры от возможной реализации информационных угроз со стороны поставщиков услуг;

управление риском технологической зависимости функционирования своих объектов информационной инфраструктуры от поставщиков услуг.

1.8. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны принимать организационные и технические меры, направленные на проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов своей готовности противостоять реализации информационных угроз в отношении критичной архитектуры.

1.9. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны принимать организационные и технические меры в отношении субъектов доступа, являющихся работниками указанных некредитных финансовых организаций и работниками поставщиков услуг, привлекаемых в рамках выполнения технологических процессов, предусмотренных в приложении к настоящему Положению, направленные на управление риском реализации информационных угроз, обусловленным возможностью несанкционированного использования предоставленных указанным субъектам доступа полномочий.

1.10. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны обеспечивать

выполнение следующих требований в отношении обеспечения своей осведомленности об актуальных информационных угрозах:

организацию взаимодействия с иными участниками технологического процесса при обмене информацией об актуальных сценариях реализации информационных угроз;

использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения непрерывного оказания финансовых услуг.

1.11. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны обеспечить управление риском возникновения зависимости обеспечения операционной надежности от субъектов доступа – работников указанных некредитных финансовых организаций, обладающих знаниями, опытом и компетенцией, которые отсутствуют у всех иных работников указанных некредитных финансовых организаций.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны обеспечить защиту критичной архитектуры от возможной реализации информационных угроз в периоды выполнения работниками указанных некредитных финансовых организаций трудовой функции дистанционно.

1.12. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, информация о признании которых системно значимыми инфраструктурными организациями финансового рынка размещается Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») и которые являются субъектами критической информационной инфраструктуры в соответствии с пунктом 8

статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), должны выполнять требования, направленные на противодействие целевым компьютерным атакам, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в зависимости от уровня опасности.

1.13. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны установить во внутренних документах описание следующих мер, направленных на реализацию требований к операционной надежности:

определение и описание состава процедур, направленных на выполнение требований к операционной надежности;

определение организационной структуры некредитной финансовой организации, задействованной в выполнении требований к операционной надежности, включающее установление функций подразделений некредитной финансовой организации (в том числе в части принятия решений, касающихся выполнения требований к операционной надежности, с обеспечением исключения конфликта интересов) и обеспечивающее контроль за выполнением требований к операционной надежности в рамках порядка организации и осуществления некредитной финансовой организацией внутреннего контроля (в случае его наличия);

выделение ресурсного обеспечения для выполнения требований к операционной надежности;

порядок утверждения и условия пересмотра процедур, направленных на выполнение требований к операционной надежности.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации,

должны обеспечить реализацию требований к операционной надежности начиная с разработки и планирования внедрения технологических процессов, указанных в приложении к настоящему Положению.

1.14. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны:

моделировать информационные угрозы в отношении критичной архитектуры;

планировать применение организационных и технических мер, направленных на реализацию требований к операционной надежности, на основе результатов оценки риска реализации информационных угроз в рамках системы управления рисками (при наличии);

обеспечивать реализацию требований к операционной надежности на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации своих объектов информационной инфраструктуры;

обеспечивать контроль соблюдения требований к операционной надежности в отношении элементов критичной архитектуры.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны устанавливать во внутренних документах порядок регистрации событий операционного риска, связанных с нарушением операционной надежности. По каждому событию операционного риска, связанному с нарушением операционной надежности, некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, должны обеспечивать регистрацию:

данных, используемых для фиксации отклонения от значений целевых показателей операционной надежности, указанных в пункте 1.3 настоящего

Положения;

данных, позволяющих выявить причину отклонения от значений целевых показателей операционной надежности, указанных в пункте 1.3 настоящего Положения;

результата реагирования на событие операционного риска, связанное с нарушением операционной надежности (принятых мер и проведенных мероприятий по реагированию на выявленное некредитной финансовой организацией или Банком России событие операционного риска, связанное с нарушением операционной надежности).

1.15. Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации, в рамках обеспечения операционной надежности должны информировать Банк России:

о выявленных событиях операционного риска, связанных с нарушением операционной надежности, включенных в перечень типов событий операционного риска, связанных с нарушением операционной надежности, размещаемый Банком России на официальном сайте Банка России в сети «Интернет» (в случае превышения допустимой доли деградации технологических процессов), а также о принятых мерах и проведенных мероприятиях по реагированию на указанные события операционного риска, связанные с нарушением операционной надежности, выявленные некредитной финансовой организацией или Банком России;

о планируемых публичных мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети «Интернет», в отношении событий операционного риска, связанных с нарушением операционной надежности, не позднее одного рабочего дня до проведения мероприятия.

Некредитные финансовые организации, обязанные соблюдать усиленный, стандартный или минимальный уровень защиты информации,

должны представлять в Банк России указанные в абзацах втором и третьем настоящего пункта сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия некредитных финансовых организаций, обязанных соблюдать усиленный, стандартный или минимальный уровень защиты информации, с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России указанные некредитные финансовые организации должны предоставлять в Банк России сведения с использованием резервного способа взаимодействия. Информация о технической инфраструктуре (автоматизированной системе) Банка России, резервном способе взаимодействия, форме и сроках направления сведений размещается на официальном сайте Банка России в сети «Интернет».

1.16. Некредитные финансовые организации, не указанные в абзаце первом пункта 1.2 настоящего Положения, в рамках обеспечения операционной надежности должны выполнять следующие требования:

проводить не реже одного раза в три года в рамках системы управления рисками (при наличии) анализ необходимости обеспечения непревышения порогового уровня допустимого времени простоя и (или) деградации технологических процессов, соблюдения значений целевых показателей операционной надежности;

закреплять по итогам указанного в абзаце втором настоящего пункта анализа в своих внутренних документах перечень технологических процессов, пороговые уровни допустимого времени простоя и (или) деградации технологических процессов, а также значения целевых показателей операционной надежности либо принимать мотивированное решение об отсутствии необходимости в обеспечении непревышения порогового уровня допустимого времени простоя и (или) деградации технологических процессов, соблюдения значений целевых показателей операционной надежности;

обеспечивать контроль за соблюдением предусмотренных своими внутренними документами пороговых уровней допустимого времени простоя и (или) деградации технологических процессов и значений целевых показателей операционной надежности (в случае их закрепления в своих внутренних документах).

Глава 2. Особенности обеспечения операционной надежности при осуществлении деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператора обмена цифровых финансовых активов

2.1. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов в целях обеспечения операционной надежности в дополнение к установленным пунктами 1.1–1.15 настоящего Положения требованиям к операционной надежности, в рамках выпуска и обращения цифровых финансовых активов должны обеспечивать выполнение следующих мероприятий:

обеспечение безопасности программной среды исполнения сделки, указанной в части 2 статьи 4 Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (Собрание законодательства Российской Федерации, 2020, № 31, ст. 5018), в том числе настройки программной среды исполнения указанной сделки, обеспечивающей функциональность программной среды в условиях сбоя при обработке данных, установление ограничений на доступ к системным ресурсам, оперативной памяти и файловой системе для программной среды исполнения указанной сделки;

применение механизмов, реализующих обработку информационных угроз, связанных с недоступностью функций компонентов информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также недоступностью функций удостоверяющего центра, указанного в статье 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2020, № 26, ст. 3997), и (или) функций иных информационных систем, взаимодействующих с информационной системой, в которой осуществляется выпуск цифровых финансовых активов.

2.2. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов в целях обеспечения операционной надежности в дополнение к установленным пунктами 1.1–1.15 настоящего Положения требованиям к операционной надежности в рамках выпуска и обращения цифровых финансовых активов в информационной системе на основе распределенного реестра должны обеспечивать выполнение следующих мероприятий:

анализ и применение алгоритмов, сохраняющих свою функциональность в условиях сбоя и обеспечивающих тождественность информации во всех базах данных, составляющих распределенный реестр, в части предотвращения включения (подмены) блоков данных с целью защиты от деструктивного воздействия на информационную систему на основе распределенного реестра, временная синхронизация проводимых финансовых операций с целью присвоения действительной временной метки;

применение механизмов, реализующих защиту от угрозы нарушения маршрутизации узлов информационной системы на основе распределенного реестра, включая механизм защиты от формирования альтернативных цепочек блоков данных в информационной системе на основе распределенного реестра, механизмы электронной подписи, позволяющие узлам

информационной системы на основе распределенного реестра обеспечивать целостность данных;

применение механизмов, реализующих систему защиты от информационных угроз, направленных на отказ в обслуживании на уровне вычислительной сети, включая механизмы, обеспечивающие непрерывную работу информационной системы на основе распределенного реестра при росте количества проводимых финансовых операций, механизмы, реализующие систему защиты от информационных угроз, направленных на задержку доставки блоков данных к узлам информационной системы на основе распределенного реестра.

Глава 3. Заключительные положения

3.1. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 22 октября 2021 года № ПСД-26) вступает в силу с 1 октября 2022 года.

3.2. Настоящее Положение применяется:

некредитными финансовыми организациями, указанными в абзаце первом пункта 1.2 настоящего Положения, обязанными соблюдать усиленный или стандартный уровень защиты информации в соответствии с подпунктом 1.4.2 или 1.4.3 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П, а также некредитными финансовыми организациями, не указанными в абзаце первом пункта 1.2 настоящего Положения, – с 1 октября 2022 года;

некредитными финансовыми организациями, указанными в абзаце первом пункта 1.2 настоящего Положения, обязанными соблюдать минимальный уровень защиты информации в соответствии с подпунктом 1.4.4 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П, – с 1 января 2023 года.

3.3. Со дня вступления в силу настоящего Положения признать утратившим силу Указание Банка России от 23 декабря 2020 года № 5673-У «О требованиях к операционной надежности при совершении финансовых сделок с использованием финансовой платформы», зарегистрированное Министерством юстиции Российской Федерации 3 февраля 2021 года № 62358.

Председатель
Центрального банка
Российской Федерации

Э.С. Набиуллина

Приложение
к Положению Банка России
от 15 ноября 2021 года № 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)»

Пороговый уровень допустимого времени простоя и (или) деградации
технологических процессов некредитных финансовых организаций

№ п/п	Некредитные финансовые организации в разрезе видов деятельности на финансовом рынке, наименование технологического процесса	Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов (в часах)	
		некредитные финансовые организации, обязанные соблюдать усиленный или стандартный уровень защиты информации в соответствии с подпунктом 1.4.2 или 1.4.3 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П	некредитные финансовые организации, обязанные соблюдать минимальный уровень защиты информации в соответствии с подпунктом 1.4.4 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П
1	2	3	4
1. Некредитные финансовые организации, осуществляющие брокерскую деятельность			
1.1	Технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами	2	4
1.2	Технологический процесс, обеспечивающий внесение записей во внутренний учет	12	12
1.3	Технологический процесс, обеспечивающий возврат клиентам денежных средств	24	24
2. Некредитные финансовые организации, осуществляющие дилерскую деятельность			
2.1	Технологический процесс, обеспечивающий совершение сделок купли-продажи ценных бумаг от своего имени и за свой счет путем	24	24

1	2	3	4
	публичного объявления цен покупки и (или) продажи определенных ценных бумаг с обязательством покупки и (или) продажи этих ценных бумаг по объявленным лицом, осуществляющим указанную деятельность, ценам		
2.2	Технологический процесс, обеспечивающий внесение записей во внутренний учет	12	12
3. Некредитные финансовые организации, осуществляющие деятельность форекс-дилера			
3.1	Технологический процесс, обеспечивающий заключение от своего имени и за свой счет с физическими лицами, не являющимися индивидуальными предпринимателями, не на организованных торгах договоров, указанных в пункте 1 статьи 4 ¹ Федерального закона от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг» (Собрание законодательства Российской Федерации, 1996, № 17, ст. 1918; 2015, № 1, ст. 13)	X	2
3.2	Технологический процесс, обеспечивающий внесение записей во внутренний учет	X	12
3.3	Технологический процесс, обеспечивающий возврат клиентам денежных средств	X	24
4. Некредитные финансовые организации, осуществляющие деятельность по управлению ценными бумагами			
4.1	Технологический процесс, обеспечивающий совершение сделок с ценными бумагами и (или) заключение договоров, являющихся производными финансовыми инструментами, в интересах учредителя управления	4	4
4.2	Технологический процесс, обеспечивающий внесение записей во внутренний учет	12	12
4.3	Технологический процесс, обеспечивающий возврат клиентам денежных средств	24	24
5. Некредитные финансовые организации, осуществляющие деятельность регистратора			
5.1	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг	24	24
5.2	Технологический процесс, обеспечивающий осуществление регистратором сверки учитываемых регистратором прав на ценные бумаги с центральным депозитарием по счету номинального держателя центрального депозитария	4	4
6. Некредитные финансовые организации, осуществляющие депозитарную деятельность, включая деятельность центрального депозитария			
6.1	Технологический процесс, обеспечивающий внесение учетных записей в учетные регистры	24	24
6.2	Технологический процесс, обеспечивающий осуществление расчетным депозитарием расчетов по результатам сделок, совершенных на организованных торгах	2	2

1	2	3	4
6.3	Технологический процесс, обеспечивающий выплату депоненту доходов в денежной форме по ценным бумагам, учет прав на которые осуществляет депозитарий, и иных причитающихся владельцам указанных ценных бумаг денежных выплат	24	24
6.4	Технологический процесс, обеспечивающий осуществление центральным депозитарием сверки учитываемых центральным депозитарием прав на ценные бумаги с регистратором по счету номинального держателя центрального депозитария	4	X
7. Некредитные финансовые организации, осуществляющие деятельность управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда (далее при совместном упоминании – фонды)			
7.1	Технологический процесс, обеспечивающий доверительное управление имуществом фондов, в том числе осуществление прав, удостоверенных ценными бумагами, составляющими имущество фондов	X	2
7.2	Технологический процесс, обеспечивающий реализацию прав владельцев инвестиционных паев	X	24
7.3	Технологический процесс, обеспечивающий осуществление учета имущества фондов и контроля за распоряжением им, в том числе процесс взаимодействия со специализированным депозитарием	X	24
8. Некредитные финансовые организации, осуществляющие деятельность специализированных депозитариев фондов			
8.1	Технологический процесс, обеспечивающий осуществление специализированным депозитарием контроля за распоряжением имуществом фондов	24	24
8.2	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг (в случае оказания услуг по ведению реестра владельцев инвестиционных паев паевых инвестиционных фондов, ипотечных сертификатов участия)	24	24
9. Некредитные финансовые организации, осуществляющие клиринговую деятельность и деятельность центрального контрагента			
9.1	Технологический процесс, обеспечивающий определение подлежащих исполнению обязательств	2	X
9.2	Технологический процесс, обеспечивающий совершение действий, направленных на исполнение подлежащих исполнению обязательств	2	X
9.3	Технологический процесс, обеспечивающий направление поручения на возврат имущества, являющегося клиринговым обеспечением	2	X
10. Некредитные финансовые организации, осуществляющие деятельность организатора торговли			

1	2	3	4
10.1	Технологический процесс, обеспечивающий заключение договора между участниками торгов	2	X
10.2	Технологический процесс, обеспечивающий ведение реестра участников торгов и их клиентов, реестра заявок, реестра заключенных на организованных торгах договоров, реестра внебиржевых договоров	2	X
10.3	Технологический процесс, обеспечивающий раскрытие и предоставление информации организатором торговли	2	X
11. Некредитные финансовые организации, осуществляющие репозитарную деятельность			
11.1	Технологический процесс, обеспечивающий учет заключенных не на организованных торгах договоров репо, договоров, являющихся производными финансовыми инструментами, а также иных договоров	12	X
11.2	Технологический процесс, обеспечивающий учет регистратором финансовых транзакций информации о совершении финансовых сделок и об операциях по ним с использованием финансовой платформы	2	X
11.3	Технологический процесс, обеспечивающий передачу (предоставление) реестра, ведение которого осуществляет репозитарий, в Банк России или в другой репозитарий	6	X
12. Некредитные финансовые организации, осуществляющие деятельность субъектов страхового дела			
12.1	Технологический процесс, обеспечивающий учет страховых случаев	24	24
12.2	Технологический процесс, обеспечивающий возврат страховой премии	24	24
12.3	Технологический процесс, обеспечивающий работу сайтов в части размещения информации, предусмотренной пунктом 6 статьи 6 Закона Российской Федерации от 27 ноября 1992 года № 4015-1 «Об организации страхового дела в Российской Федерации» (Собрание законодательства Российской Федерации 1993, № 2, ст. 56; 2021, № 27, ст. 5171)	24	24
13. Некредитные финансовые организации, осуществляющие деятельность негосударственных пенсионных фондов			
13.1	Технологический процесс, обеспечивающий осуществление выплат вкладчикам, участникам, застрахованным лицам и их правопреемникам негосударственного пенсионного фонда в рамках обязательного пенсионного страхования и негосударственного пенсионного обеспечения	24	X
13.2	Технологический процесс, обеспечивающий передачу средств пенсионных резервов и	24	X

1	2	3	4
	пенсионных накоплений управляющей компании		
13.3	Технологический процесс, обеспечивающий перевод выкупных сумм (средств пенсионных накоплений) в иные негосударственные пенсионные фонды и Пенсионный фонд Российской Федерации	24	X
13.4	Технологический процесс, обеспечивающий размещение средств пенсионных резервов	24	X
13.5	Технологический процесс, обеспечивающий расторжение договора негосударственного пенсионного обеспечения, договора об обязательном пенсионном страховании с негосударственным пенсионным фондом	24	X
14. Некредитные финансовые организации, осуществляющие деятельность операторов инвестиционных платформ			
14.1	Технологический процесс, обеспечивающий предоставление доступа к инвестиционной платформе	24	X
14.2	Технологический процесс, обеспечивающий размещение инвестиционного предложения	24	X
14.3	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем предоставления займов	24	X
14.4	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы	24	X
14.5	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения утилитарных цифровых прав	24	X
14.6	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения цифровых финансовых активов	24	X
15. Некредитные финансовые организации, осуществляющие деятельность операторов финансовых платформ			
15.1	Технологический процесс, обеспечивающий возможность совершения участниками финансовой платформы финансовых сделок с использованием финансовой платформы	2	4
16. Некредитные финансовые организации, осуществляющие деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов			
16.1	Технологический процесс, обеспечивающий доступ к информационной системе, в том числе ведение реестра пользователей информационной системы	6	12

1	2	3	4
16.2	Технологический процесс, обеспечивающий выпуск цифровых финансовых активов в информационной системе	24	24
16.3	Технологический процесс, обеспечивающий обращение цифровых финансовых активов в информационной системе, в том числе погашение записей о цифровых финансовых активах	6	12
16.4	Технологический процесс, обеспечивающий внесение записей оператором информационной системы в соответствии с частью 2 статьи 6 Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (Собрание законодательства Российской Федерации, 2020, № 31, ст. 5018)	2	4
16.5	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев акций непубличных акционерных обществ, осуществляющих выпуск цифровых финансовых активов, удостоверяющих права участия в капитале указанных непубличных акционерных обществ	24	24
16.6	Технологический процесс, обеспечивающий взаимодействие с оператором обмена цифровых финансовых активов	6	12
16.7	Технологический процесс, обеспечивающий мониторинг тождественности информации, содержащейся во всех базах данных, составляющих распределенный реестр	6	12
17. Некредитные финансовые организации, осуществляющие деятельность операторов обмена цифровых финансовых активов			
17.1	Технологический процесс, обеспечивающий возможность совершения сделок с цифровыми финансовыми активами	6	12
17.2	Технологический процесс, обеспечивающий взаимодействие с оператором информационной системы	6	12