Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«___» _____ 2021 г. №_____ -П

г. Москва

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)

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 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 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), а также требования к операционной надежности к оператору информационной системы, в которой осуществляется выпуск цифровых финансовых активов, к деятельности операторов обмена цифровых финансовых активов.

Глава 1. Обязательные для некредитных финансовых организаций требования 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)

1.1. Некредитные финансовые организации, в том числе операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторы обмена цифровых финансовых активов (далее – некредитные финансовые организации), должны выполнять требования 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)», с использованием автоматизированных систем путем обеспечения непрерывности оказания финансовых услуг в условиях возникновения информационных угроз.

1.2. Некредитные финансовые организации, указанные в приложении к настоящему Положению, должны обеспечить пороговый уровень допустимого времени простоя технологических процессов, обеспечивающих

осуществление деятельности в сфере финансовых рынков, указанных в приложении к настоящему Положению (далее – технологические процессы), и (или) нарушения технологических процессов, приводящего к неоказанию или ненадлежащему оказанию финансовых услуг (далее – деградация технологических процессов), в соответствии с приложением к настоящему Положению.

Некредитные финансовые организации, не указанные в приложении к настоящему Положению, самостоятельно устанавливают и обеспечивают пороговый уровень допустимого времени простоя и (или) деградации технологических процессов, не указанных в приложении к настоящему Положению, и иные показатели операционной надежности.

1.3. Некредитные финансовые организации должны определить во внутренних документах для каждого технологического процесса значения следующих целевых показателей операционной надежности:

допустимого отношения общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события или серии связанных событий, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг (далее – инцидент операционной надежности) к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг, рассчитанное некредитной финансовой организацией на основе статистических данных за период не менее двенадцати календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности (далее – допустимая доля деградации технологических процессов);

допустимого времени простоя и (или) деградации технологического процесса в рамках инцидента операционной надежности (в случае отклонения от 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 отклонения от допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу календарного месяца;

установленный режим работы (функционирования) технологического процесса.

В случаях превышения допустимого времени простоя и (или) деградации технологических процессов, а также отклонения от допустимой доли деградации технологических процессов некредитные финансовые организации должны обеспечить во внутренних документах фиксацию:

фактического времени простоя и (или) деградации технологического процесса, исчисляемого по каждому инциденту операционной надежности;

фактической доли деградации технологического процесса в рамках отдельного инцидента операционной надежности;

суммарного времени простоя и (или) деградации технологического процесса за последние двенадцать календарных месяцев.

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.

1.4. Некредитные финансовые организации должны определить значения целевых показателей операционной надежности и обеспечить контроль за их соблюдением. В случае, если законодательством Российской Федерации установлена обязательность наличия у некредитной финансовой организации системы управления рисками, то такая некредитная финансовая организация должна выполнить требования настоящего абзаца в рамках системы управления рисками.

Некредитная финансовая организация должна не реже одного раза в год проводить анализ необходимости пересмотра значений целевых показателей

операционной надежности.

1.5. Некредитные финансовые организации должны выполнять требования к операционной надежности при осуществлении деятельности в сфере финансовых рынков, которые включают в себя:

требования к определению значений целевых показателей операционной надежности и обеспечению контроля за их соблюдением;

требования в отношении идентификации состава элементов, указанных в подпункте 1.6 настоящего пункта (далее – критичная архитектура);

требования в отношении управления изменениями критичной архитектуры;

требования в отношении выявления, регистрации инцидентов операционной надежности и реагирования на них, а также восстановления выполнения технологических процессов и функционирования программно-аппаратных средств после реализации указанных инцидентов;

требования в отношении взаимодействия с внешними контрагентами, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов (далее – поставщики услуг);

требования в отношении тестирования операционной надежности технологических процессов;

требования в отношении управления риском несанкционированного доступа работников некредитной финансовой организации или работников поставщиков услуг, обладающих полномочиями доступа к программно-аппаратным средствам (далее – внутренний нарушитель), к программно-аппаратным средствам;

требования в отношении обеспечения осведомленности некредитной финансовой организации об актуальных информационных угрозах;

иные требования в соответствии с пунктами 1.7–1.11 настоящего

Положения.

1.6. Некредитные финансовые организации в отношении идентификации критичной архитектуры должны обеспечивать организацию учета и мониторинга следующих элементов критичной архитектуры:

технологических процессов, реализуемых непосредственно некредитной финансовой организацией;

технологических процессов, реализуемых поставщиками услуг;

подразделений (работников) некредитной финансовой организации, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов (далее – подразделения некредитной финансовой организации);

технологических участков (этапов) технологических процессов;

программно-аппаратных средств некредитной финансовой организации, задействованных при выполнении каждого технологического процесса;

работников некредитной финансовой организации или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к программно-аппаратным средствам (далее – субъекты доступа), задействованных при выполнении каждого технологического процесса;

взаимосвязей и взаимозависимостей между некредитными финансовыми организациями, а также поставщиками услуг в рамках выполнения технологических процессов (далее при совместном упоминании – участники технологического процесса), в том числе взаимосвязей и взаимозависимостей между их программно-аппаратными средствами;

программно-аппаратных средств поставщиков услуг, задействованных при выполнении технологических процессов;

каналов передачи информации, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса при взаимодействии с работниками некредитной финансовой организации.

1.6.1. Некредитные финансовые организации должны обеспечивать выполнение следующих требований в отношении управления изменениями критичной архитектуры:

предотвращение возникновения уязвимостей в критичной архитектуре, с использованием которых могут реализоваться информационные угрозы, и которые могут повлечь превышение (отклонение от) значений целевых показателей операционной надежности;

планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение недопустимости неоказания или ненадлежащего оказания финансовых услуг;

управление конфигурациями программно-аппаратных средств;

управление уязвимостями и обновлениями (исправлениями) программно-аппаратных средств.

1.6.2. Некредитные финансовые организации должны обеспечивать выполнение следующих требований в отношении выявления, регистрации инцидентов операционной надежности и реагирования на них, а также восстановления выполнения технологических процессов и функционирования программно-аппаратных средств после реализации таких инцидентов:

выявление и регистрацию инцидентов операционной надежности, в том числе обнаружение компьютерных атак и фактов воздействия вредоносного кода на программно-аппаратные средства;

реагирование на инциденты операционной надежности в отношении критичной архитектуры;

восстановление функционирования технологических процессов и программно-аппаратных средств после реализации инцидентов операционной надежности;

проведение анализа причин и последствий реализации инцидентов операционной надежности;

организацию взаимодействия между подразделениями некредитной

финансовой организации, а также между некредитной финансовой организацией и Банком России, иными участниками технологического процесса в рамках реагирования на инциденты операционной надежности и восстановления выполнения технологических процессов и функционирования программно-аппаратных средств после реализации инцидентов операционной надежности.

1.6.3. Некредитные финансовые организации должны обеспечивать выполнение следующих требований в отношении взаимодействия с поставщиками услуг:

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 некредитной финансовой организации от поставщиков услуг;

предотвращение возможной реализации информационных угроз при сопровождении и техническом обслуживании программно-аппаратных средств некредитной финансовой организации поставщиками услуг.

1.6.4. Некредитные финансовые организации в отношении тестирования операционной надежности технологических процессов должны принимать организационные и технические меры, направленные на разработку сценарного анализа и проведение с использованием сценарного анализа тестирования готовности некредитной финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры.

1.6.5. Некредитные финансовые организации в отношении управления риском несанкционированного доступа внутреннего нарушителя к программно-аппаратным средствам должны принимать организационные и

технические меры в отношении субъектов доступа, являющихся работниками некредитной финансовой организации и работниками поставщиков услуг, привлекаемых в рамках выполнения технологических процессов, направленные на управление риском реализации информационных угроз, обусловленным возможностью несанкционированного использования предоставленных указанным субъектам доступа полномочий.

1.6.6. Некредитные финансовые организации должны обеспечивать выполнение следующих требований в отношении обеспечения осведомленности об актуальных информационных угрозах:

организацию взаимодействия некредитной финансовой организации и иных участников 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.

1.7. Некредитная финансовая организация должна обеспечить управление риском возникновения зависимости обеспечения операционной надежности от субъектов доступа – работников некредитной финансовой организации, обладающих уникальными знаниями, опытом и компетенцией, а также защиту критичной архитектуры от возможной реализации информационных угроз при организации дистанционной работы работников некредитной финансовой организации.

1.8. Некредитные финансовые организации, являющиеся системно значимыми инфраструктурными организациями финансового рынка, указанными в постановлении Правительства Российской Федерации от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их

значений» (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204), по требованию Банка России должны обеспечить:

реализацию мер противодействия целевым компьютерным атакам;

моделирование сценариев компьютерных атак, проведение плановых тренировок (учений) по проверке готовности к действиям при установлении уровня опасности проведения целевых компьютерных атак;

внеплановую оценку защищенности критичной архитектуры и устранение выявленных недостатков;

оперативное взаимодействие подразделений некредитных финансовых организаций, указанных в абзаце первом настоящего пункта, функционирующих в оперативном режиме работы, с Банком России.

1.9. Некредитная финансовая организация должна установить во внутренних документах описание мер, направленных на реализацию требований к операционной надежности, установленных настоящим Положением, включая:

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, в том числе обеспечивающее установление функций подразделений некредитной финансовой организации (в том числе в части принятия решений, связанных с выполнением требований к операционной надежности, с учетом исключения конфликта интересов) и контроль за выполнением требований к операционной надежности в рамках порядка организации и осуществления некредитной финансовой организацией внутреннего контроля (в случае наличия);

выделение ресурсного обеспечения для выполнения требований к операционной надежности;

порядок утверждения и условия пересмотра процедур, направленных на

выполнение требований к операционной надежности.

Некредитная финансовая организация должна обеспечить реализацию требований к операционной надежности начиная с разработки и планирования внедрения технологических процессов.

1.10. В целях реализации требований к операционной надежности некредитная финансовая организация должна:

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;

обеспечивать реализацию требований к операционной надежности на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации программно-аппаратных средств;

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

Некредитные финансовые организации должны устанавливать во внутренних документах порядок регистрации инцидентов операционной надежности. По каждому инциденту операционной надежности некредитные финансовые организации должны обеспечивать регистрацию:

данных, используемых для фиксации превышения (отклонения от) значений установленных целевых показателей операционной надежности;

данных, позволяющих выявить причину превышения (отклонения от) значений установленных целевых показателей операционной надежности;

результата реагирования на инцидент операционной надежности (о принятых мерах и проведенных мероприятиях по реагированию на выявленный некредитной финансовой организацией или Банком России

инцидент операционной надежности).

1.11. Некредитные финансовые организации должны информировать Банк России:

о выявленных инцидентах операционной надежности, включенных в перечень типов инцидентов операционной надежности, размещаемый Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный некредитной финансовой организацией или Банком России инцидент операционной надежности;

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

Некредитные финансовые организации должны предоставлять в Банк России указанные во втором и третьем абзацах настоящего пункта сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия некредитной финансовой организации с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России 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».

Глава 2. **Требования к операционной надежности к оператору информационной системы, в которой осуществляется**

выпуск цифровых финансовых активов, к деятельности операторов обмена цифровых финансовых активов

2.1. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов в дополнение к установленным пунктами 1.1 – 1.11 настоящего Положения требованиям к операционной надежности, а также пунктом 3.2 Положения Банка России от ___ №___ «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 ___ №___, в рамках выпуска и обращения цифровых финансовых активов должны обеспечивать выполнение следующих мероприятий:

обеспечение безопасности виртуальной среды выполнения 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) (далее – Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»), в том числе обеспечение корректной настройки виртуальной среды совершения сделки, указанной в части 2 статьи 4 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», с целью достижения отказоустойчивости обработки данных, определение и установление ограничений на доступ к системным ресурсам, оперативной памяти и файловой системе для виртуальной среды совершения

сделки, указанной в части 2 статьи 4 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»;

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 и (или) функций иных централизованных 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 дополнение к установленным пунктами 1.1 – 1.11 настоящего Положения требованиям к операционной надежности, а также пунктом 3.3 Положения Банка России от ___ №___ «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 ___ №___, в рамках выпуска и обращения цифровых финансовых активов в информационной системе на основе распределенного реестра должны обеспечивать выполнение следующих мероприятий:

анализ и применение отказоустойчивых алгоритмов, обеспечивающих тождественность информации во всех базах данных, составляющих распределенный реестр, включая предотвращение включения (подмены) блоков данных с целью защиты от деструктивного воздействия на информационную систему на основе распределенного реестра, временную синхронизацию проводимых операций с целью присвоения действительной и согласованной временной метки;

применение механизмов, реализующих защиту от угрозы нарушения маршрутизации узлов, включая реализацию механизма защиты от формирования альтернативных цепочек блоков данных в информационной системе на основе распределенного реестра, реализацию механизмов электронной подписи, позволяющих узлам информационной системы на основе распределенного реестра обеспечивать целостность данных;

применение механизмов, реализующих систему защиты от атак, направленных на отказ в обслуживании на уровне вычислительной сети, включая применение механизмов, обеспечивающих непрерывную работу информационной системы на основе распределенного реестра при росте количества проводимых операций, реализацию механизмов, реализующих систему защиты от атак, направленных на задержку доставки блоков данных к узлам информационной системы на основе распределенного реестра.

Глава 3. **Заключительные положения**

3.1. Действие настоящего Положения не распространяется на операторов финансовых платформ.

3.2. Центральные контрагенты должны определять целевые показатели операционной надежности с учетом требований Положения Банка России от 30 декабря 2016 года № 575-П «О требованиях к управлению рисками, правилам организации системы управления рисками, клиринговому обеспечению, размещению имущества, формированию активов центрального контрагента, а также к кругу лиц, в которых центральный контрагент имеет право открывать торговые и клиринговые счета, и методике определения выделенного капитала центрального контрагента», зарегистрированного в Министерстве юстиции Российской Федерации 20 марта 2017 года № 46034, а также Указания Банка России от 30 декабря 2016 года № 4258-У «О требованиях к содержанию, порядке и сроках представления в Банк России плана обеспечения непрерывности деятельности центрального контрагента,

изменений, вносимых в него, о порядке оценки плана обеспечения непрерывности деятельности центрального контрагента, о требованиях к программно-техническим средствам и сетевым коммуникациям центрального контрагента, а также о порядке создания, ведения и хранения баз данных, содержащих информацию об имуществе, обязательствах центрального контрагента и их движении», зарегистрированного в Министерстве юстиции Российской Федерации 15 февраля 2017 года № 45648.

Репозитарии должны определять целевые показатели операционной надежности с учетом требований Указания Банка России от 6 октября 2016 года № 4148-У «О требованиях к разработке и утверждению плана обеспечения непрерывности деятельности репозитария и плана обеспечения финансовой устойчивости репозитария», зарегистрированного в Министерстве юстиции Российской Федерации 28 октября 2016 года № 44179.

Организаторы торговли, центральные депозитарии должны обеспечивать идентификацию критичной архитектуры, управление изменениями критичной архитектуры, выявление, регистрацию инцидентов операционной надежности и реагирование на них, а также восстановление выполнения технологических процессов и функционирования программно-аппаратных средств после реализации указанных инцидентов, взаимодействие с поставщиками услуг, тестирование операционной надежности технологических процессов, управление риском внутреннего нарушителя, осведомленность об актуальных информационных угрозах, предоставление в Банк России указанных в пункте 1.11 настоящего Положения сведений с учетом соответственно требований Указания Банка России от 7 мая 2018 года № 4791-У «О требованиях к организации организатором торговли системы управления рисками, связанными с организацией торгов, а также с осуществлением операций с собственным имуществом, и к документам организатора торговли, определяющим меры, направленные на снижение

указанных рисков и предотвращение конфликта интересов», зарегистрированного в Министерстве юстиции Российской Федерации 17 сентября 2018 года № 52176, Указания Банка России от 12 сентября 2018 года № 4905-У «О требованиях к деятельности центрального депозитария в части организации управления рисками, связанными с осуществлением деятельности центрального депозитария, а также к правилам управления рисками, связанными с осуществлением деятельности центрального депозитария», зарегистрированного в Министерстве юстиции Российской Федерации 16 ноября 2018 года № 52702.

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

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Положению Банка России от ___ №___ «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)»

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

№	Наименование деятельности в сфере финансовых рынков, технологического процесса	Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов	
		Некредитные финансовые организации, обязанные соблюдать усиленный или стандартный уровень защиты информации[1]	Некредитные финансовые организации, обязанные соблюдать минимальный уровень защиты информации[2], а также иные некредитные финансовые организации
Брокерская деятельность			
	Технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами	2 ч.	4 ч.
	Технологический процесс, обеспечивающий внесение записей во внутренней учет	2 ч.	4 ч.
	Технологический процесс, обеспечивающий возврат клиентам денежных средств	24 ч.	24 ч.
	Дилерская деятельность		
	Технологический процесс, обеспечивающий совершение сделок купли-продажи ценных бумаг от своего	2 ч.	2 ч.

[1] В соответствии с требованиями, установленными Банком России на основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

[2] В соответствии с требованиями, установленными Банком России на основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

	имени и за свой счет путем публичного объявления цен покупки и/или продажи определенных ценных бумаг с обязательством покупки и/или продажи этих ценных бумаг по объявленным лицом, осуществляющим такую деятельность, ценам.		
	Технологический процесс, обеспечивающий внесение записей во внутренней учет	2 ч.	2 ч.
Деятельность форекс-дилера			
	Технологический процесс, обеспечивающий заключение от своего имени и за свой счет с физическими лицами, не являющимися индивидуальными предпринимателями, не на организованных торгах сделок, перечисленных в ст. 4.1 39-ФЗ	Х	2 ч.
	Технологический процесс, обеспечивающий внесение записей во внутренней учет	Х	2 ч
	Технологический процесс, обеспечивающий возврат клиентам денежных средств	Х	24 ч
Деятельность по управлению ценными бумагами			
	Технологический процесс, обеспечивающий совершения сделок с ценными бумагами и (или) заключения договоров, являющихся производными финансовыми инструментами в интересах учредителя управления	2 ч.	4 ч.
	Технологический процесс, обеспечивающий внесение записей во внутренней учет	2 ч.	4 ч.
	Технологический процесс, обеспечивающий возврат клиентам денежных средств	24 ч.	24 ч.
Деятельность регистратора			
	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг	24 ч.	24 ч.
		24 ч.	24 ч
Депозитарная деятельность включая ЦД			
	Технологический процесс, обеспечивающий внесение учетных записей в учетные регистры	24 ч.	24 ч.
	Технологический процесс, обеспечивающий осуществление	2 ч.	2 ч.

	расчетным депозитарием расчетов по результатам сделок, совершенных на организованных торгах)		
	Технологический процесс, обеспечивающий выплату депоненту доходов в денежной форме, причитающихся владельцам ценных бумаг	24 ч.	24 ч.
	Технологический процесс обеспечивающий осуществление ЦД сверки учитываемых ЦБ с регистратором по счёту номинального держателя центрального депозитария.	4 ч.	Х
Деятельность управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда (фонды)			
	Технологический процесс, обеспечивающий доверительное управление имуществом фондов, в том числе осуществление прав, удостоверенных ценными бумагами, составляющими фонды	2 ч	4 ч.
	Технологический процесс, обеспечивающий реализацию прав владельцев инвестиционных паев	24 ч	24 ч.
	Технологический процесс, обеспечивающий осуществление учета имущества фондов и контроля за его распоряжением, в т.ч. процесс взаимодействия со специализированным депозитарием.	24 ч	24
Деятельность специализированных депозитариев инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда			
	Технологический процесс, обеспечивающий осуществление специализированным депозитарием контроля за распоряжением имуществом клиентов	24 ч.	24 ч.
Клиринговая деятельность			
	Технологический процесс, обеспечивающий определение подлежащих исполнению обязательств	2 ч.	Х
	Технологический процесс, обеспечивающий совершение действий, направленных на исполнение подлежащих исполнению обязательств	2 ч.	Х
	Технологический процесс, обеспечивающий направление поручения на возврат имущества,	2 ч.	Х

	являющегося клиринговым обеспечением		
Деятельность центрального контрагента			
	Технологический процесс, обеспечивающий заключение договора между центральным контрагентом и участником торгов / клиринга	2 ч.	X
Деятельность организатора торговли			
	Технологический процесс, обеспечивающий заключение договора между участниками торгов	2 ч.	X
	Технологический процесс, обеспечивающий ведение реестров (по 325-ФЗ «Об организованных торгах» и 437-П «О деятельности по проведению организованных торгов»)	2 ч.	X
	Технологический процесс, обеспечивающий раскрытие и предоставление информации организатора торговли	2 ч.	X
Репозитарная деятельность			
	Технологический процесс, обеспечивающий учет информации об осуществленных финансовых операциях – учет заключенных не на организованных торгах договоров репо, договоров, являющихся производными финансовыми инструментами, а также иных договоров	12 ч.	X
	Технологический процесс, обеспечивающий учет регистратором финансовых транзакций информации об осуществленных финансовых операциях - учет совершенных финансовых сделок и операций по ним с использованием финансовой платформы	2 ч.	X
	Технологический процесс, обеспечивающий передачу реестра, ведение которого осуществляет репозитарий, в Банк России или в другой репозитарий	6 ч.	
Деятельность субъектов страхового дела			
	Технологический процесс, обеспечивающий оформление договоров страхования	2 ч.	4 ч.
	Технологический процесс, обеспечивающий сопровождение договоров страхования	1 ч.	1 ч.

	Технологический процесс, обеспечивающий учет страховых случаев	24 ч.	24 ч.
	Технологический процесс, обеспечивающий изменение договоров страхования	2 ч.	4 ч.
	Технологический процесс, обеспечивающий возврат страховой премии	24 ч.	24 ч.
	Технологический процесс, обеспечивающий формирование и контроль исполнения плановых операций по договору	24 ч.	24 ч.
	Технологический процесс, обеспечивающий расчет штрафов	24 ч.	24 ч.
	Технологический процесс, обеспечивающий погашение задолженностей	24 ч.	24 ч.
	Технологический процесс, обеспечивающий автоматического прекращения договоров страхования	24 ч.	24 ч.
	Технологический процесс, обеспечивающий работу документами, отражающими движение денежных средств по договорам страхования	24 ч.	24 ч.
	Технологический процесс, обеспечивающий работу сайтов	0,1 ч.	0,1 ч.
Деятельность негосударственных пенсионных фондов			
	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 ч.	X
	Технологический процесс, обеспечивающий передачу средств пенсионных резервов и пенсионных накоплений управляющей компании	24 ч.	X
	Технологический процесс перевода выкупных сумм (средств пенсионных накоплений) в иные негосударственные пенсионные фонды и Пенсионный фонд Российской Федерации	24 ч.	X
	Технологический процесс, обеспечивающий размещение средств пенсионных резервов	24 ч.	X

	Технологический процесс, обеспечивающий расторжение договора с негосударственным пенсионным фондом	24 ч.	X
Деятельность бюро кредитных историй			
	Технологический процесс, обеспечивающий передачу источником формирования кредитной истории информации о субъекте кредитной истории в бюро кредитных историй	X	24 ч.
	Технологический процесс, обеспечивающий передачу бюро кредитных историй кредитного отчета пользователям кредитных историй	X	4 ч.
Деятельность операторов инвестиционных платформ			
	Технологический процесс, обеспечивающий предоставление доступа к инвестиционной платформе	24 ч.	X
	Технологический процесс, обеспечивающий размещение инвестиционного предложения	24 ч.	X
	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем предоставления займов	24 ч.	X
	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы	24 ч.	X
	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения утилитарных цифровых прав	24 ч.	X
	Технологический процесс обеспечивающий инвестирование путем приобретения цифровых финансовых активов	24 ч.	X
	Деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов		
	Технологический процесс, обеспечивающий доступ к информационной системе, в том числе ведение реестра пользователей информационной системы	12 ч.	6 ч.
	Технологический процесс, обеспечивающий выпуск цифровых	24 ч.	24 ч.

	финансовых активов в информационной системе		
	Технологический процесс, обеспечивающий обращение цифровых финансовых активов в информационной системе, в том числе их погашение	12 ч.	6 ч.
	Технологический процесс, обеспечивающий внесение записей оператором информационной системы в соответствии с частью 2 статьи 6 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах….»	4 ч.	2 ч.
	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев акций непубличных акционерных обществ выпущенных в виде цифровых финансовых активов	24 ч.	24 ч.
	Технологический процесс, обеспечивающий взаимодействие с оператором обмена цифровых финансовых активов	12 ч.	6 ч.
	Технологический процесс, обеспечивающий мониторинг тождественности информации, содержащейся во всех базах данных, составляющих распределенный реестр	12 ч.	6 ч.
	Технологический процесс, обеспечивающий исполнение сделок с цифровыми финансовыми активами (при наличии)	12 ч.	6 ч.
	Деятельность операторов обмена цифровых финансовых активов		
	Технологический процесс, обеспечивающий возможность совершения сделок с цифровыми финансовыми активами	12 ч.	6 ч.
	Технологический процесс, обеспечивающий взаимодействие с оператором информационной системы	12 ч.	6 ч.
	Технологический процесс, обеспечивающий исполнение сделок с цифровыми финансовыми активами (при наличии)	12 ч.	6 ч.