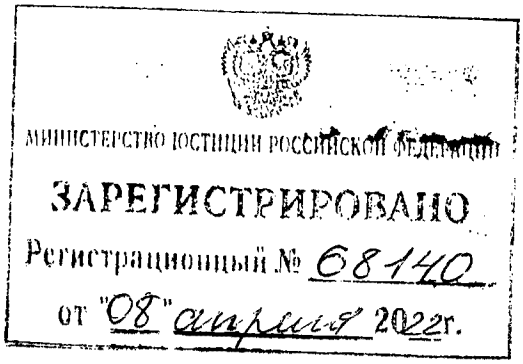
ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«12» января 2022 г. № 787-П

г. Москва



Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг

Настоящее Положение на основании статьи 57[5] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»[1] устанавливает обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг.

1. Кредитные организации, за исключением центрального контрагента в значении, установленном пунктом 17 статьи 2 Федерального закона от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте»[2], и центрального депозитария

[1] Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 1, ст. 53.
[2] Собрание законодательства Российской Федерации, 2011, № 7, ст. 904; 2016, № 1, ст. 23.

в значении, установленном в статье 2 Федерального закона от 7 декабря 2011 года № 414-ФЗ «О центральном депозитарии»[3], должны выполнять установленные настоящим Положением требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг (далее – требования к операционной надежности) с учетом требований к системе управления операционным риском, установленных Положением Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[4] (далее – Положение Банка России № 716-П). Требования к операционной надежности должны соблюдаться кредитными организациями при выполнении критически важных процессов, определенных согласно подпункту 4.1.1 пункта 4.1 Положения Банка России № 716-П в рамках системы управления операционным риском (далее – критически важные процессы), при осуществлении банковской деятельности с использованием автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее – объекты информационной инфраструктуры).

Кредитные организации должны обеспечить операционную надежность при осуществлении банковской деятельности с использованием объектов информационной инфраструктуры путем обеспечения непрерывности выполнения критически важных процессов с соблюдением контрольных показателей уровня операционного риска, устанавливаемых кредитной организацией в соответствии с пунктом 3 настоящего Положения, при возникновении отказов и (или) нарушений функционирования объектов информационной инфраструктуры, и (или) несоответствии их функциональных возможностей и характеристик потребностям кредитной организации (далее – сбои объектов

[3] Собрание законодательства Российской Федерации, 2011, № 50, ст. 7356.
[4] Зарегистрировано Минюстом России 3 июня 2020 года, регистрационный № 58577.

информационной инфраструктуры), и (или) реализации киберриска, предусмотренного абзацем вторым пункта 7.2 Положения Банка России № 716-П.

2. Кредитные организации в рамках обеспечения операционной надежности должны обеспечить непревышение значения порогового уровня допустимого времени простоя и (или) нарушения технологических процессов, обеспечивающих выполнение критически важных процессов и указанных в приложении к настоящему Положению (далее – технологические процессы), приводящих к неоказанию или ненадлежащему оказанию банковских услуг (далее – пороговый уровень допустимого времени простоя и (или) деградации технологических процессов кредитных организаций), предусмотренного приложением к настоящему Положению.

3. Кредитные организации с учетом требований главы 5 Положения Банка России № 716-П должны определить во внутренних документах для каждого технологического процесса и соблюдать значения следующих контрольных показателей уровня операционного риска для целей обеспечения операционной надежности (далее – целевые показатели операционной надежности):

допустимого отношения общего количества банковских операций и иных операций, осуществляемых в рамках технологического процесса, совершенных во время нарушений технологических процессов, приводящих к неоказанию или ненадлежащему оказанию банковских услуг (далее – деградация технологического процесса (технологических процессов), в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к неоказанию или ненадлежащему оказанию банковских услуг (далее – инцидент операционной надежности), к ожидаемому количеству

банковских операций и иных операций, осуществляемых в рамках технологических процессов, за тот же период в случае непрерывного оказания банковских услуг, установленного кредитной организацией (далее – допустимая доля деградации технологического процесса);

допустимого времени простоя и (или) деградации технологических процессов кредитных организаций в рамках инцидента операционной надежности (в случае превышения допустимой доли деградации технологического процесса). Значение данного целевого показателя устанавливается кредитной организацией не выше значений, предусмотренных приложением к настоящему Положению;

допустимого суммарного времени простоя и (или) деградации технологического процесса кредитной организации (в случае превышения допустимой доли деградации технологического процесса) в течение очередного календарного года;

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 кредитной организацией 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 кредитной организации).

В случае если технологический процесс функционирует менее двенадцати календарных месяцев, кредитные организации 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 кредитной организации).

4. В случаях превышения допустимой доли деградации технологических процессов кредитные организации должны обеспечить фиксацию:

фактического времени простоя и (или) деградации технологического процесса, исчисляемого по каждому инциденту операционной надежности (с момента нарушения технологического процесса, приводящего к неоказанию или ненадлежащему оказанию банковских услуг, в связи с возникновением события или серии связанных событий, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, до момента восстановления технологического процесса);

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 плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов и проводимых в соответствии с внутренними документами кредитных организаций.

5. Кредитные организации должны не реже одного раза в год проводить анализ необходимости пересмотра значений целевых показателей операционной надежности с учетом требований к системе контрольных показателей уровня операционного риска, определенных главой 5 Положения Банка России № 716-П.

6. Кредитные организации должны разработать во внутренних

документах и выполнять требования к операционной надежности, которые включают в себя:

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

требования к идентификации состава элементов, указанных в подпункте 6.1 настоящего пункта;

требования к управлению изменениями элементов, указанных в подпункте 6.1 настоящего пункта;

требования к выявлению, регистрации инцидентов операционной надежности и реагированию на них, а также восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации указанных инцидентов с учетом установленных главой 7 Положения Банка России № 716-П требований к выявлению событий риска информационной безопасности, порядку реагирования на выявленные события риска информационной безопасности и восстановлению деятельности кредитной организации в случае реализации таких событий;

требования к взаимодействию с третьими лицами (внешними подрядчиками, контрагентами, участниками банковской группы), оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов (далее – поставщики услуг в сфере информационных технологий), с учетом установленных главами 7 и 8 Положения Банка России № 716-П требований к управлению риском информационной безопасности и риском информационных систем при передаче поставщикам услуг в сфере информационных технологий выполнения отдельных функций кредитной организации и (или) использовании внешних информационных систем, а также требований к аутсорсингу обслуживания и функционирования информационных систем;

требования к тестированию операционной надежности технологических процессов;

требования к нейтрализации информационных угроз со стороны несанкционированного доступа работников кредитной организации или работников поставщиков услуг в сфере информационных технологий, обладающих полномочиями доступа к объектам информационной инфраструктуры (далее – внутренний нарушитель), к объектам информационной инфраструктуры;

требования к обеспечению осведомленности кредитной организации об актуальных информационных угрозах, которые могут привести к инцидентам операционной надежности.

6.1. Кредитные организации должны обеспечивать организацию учета и контроля состава следующих элементов (далее при совместном упоминании – критичная архитектура):

технологических процессов, реализуемых непосредственно кредитной организацией;

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

объектов информационной инфраструктуры кредитной организации, задействованных при выполнении каждого технологического процесса;

технологических участков технологических процессов, установленных в абзацах втором – шестом подпункта 5.2 пункта 5 Положения Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»[5] (далее соответственно – Положение Банка России № 683-П, технологические

[5] Зарегистрировано Минюстом России 16 мая 2019 года, регистрационный № 54637.

участки технологических процессов);

технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий;

работников кредитных организаций или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной инфраструктуры (далее – субъекты доступа), задействованных при выполнении каждого технологического процесса;

взаимосвязей и взаимозависимостей кредитной организации с иными кредитными организациями, некредитными финансовыми организациями, поставщиками услуг в сфере информационных технологий в рамках выполнения технологических процессов (далее при совместном упоминании – участники технологического процесса);

каналов передачи защищаемой информации, установленной в абзацах первом – пятом пункта 1 Положения Банка России № 683-П, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса.

В целях организации учета и контроля состава технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий, кредитные организации должны обеспечивать ведение отдельного реестра в соответствии с внутренними документами.

Кредитные организации в отношении элементов, указанных в подпункте 6.1 настоящего пункта, 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»[6] (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[7].

6.2. Кредитные организации должны обеспечивать выполнение следующих требований к управлению изменениями критичной архитектуры:

управление уязвимостями в критичной архитектуре, из-за которых могут реализоваться информационные угрозы и которые могут повлечь превышение значений целевых показателей операционной надежности;

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

управление конфигурациями (настраиваемыми параметрами) объектов информационной инфраструктуры;

управление уязвимостями и обновлениями (исправлениями) объектов информационной инфраструктуры.

6.3. Кредитные организации должны обеспечивать выполнение следующих требований к выявлению, регистрации инцидентов операционной надежности и реагированию на них, а также восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации таких инцидентов:

выявление и регистрация инцидентов операционной надежности;

реагирование на инциденты операционной надежности в отношении критичной архитектуры;

восстановление функционирования технологических процессов и

---

[6] Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736.
[7] Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736.

объектов информационной инфраструктуры после реализации инцидентов операционной надежности;

проведение анализа причин и последствий реализации инцидентов операционной надежности;

организация взаимодействия между подразделениями кредитной организации, а также между кредитной организацией и Банком России, иными участниками технологического процесса в рамках реагирования на инциденты операционной надежности и восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации инцидентов операционной надежности.

6.4. Кредитные организации должны обеспечивать выполнение следующих требований к взаимодействию с поставщиками услуг в сфере информационных технологий:

нейтрализация информационных угроз, связанных с привлечением поставщиков услуг в сфере информационных технологий, в том числе защита объектов информационной инфраструктуры от возможной реализации информационных угроз со стороны поставщиков услуг в сфере информационных технологий;

нейтрализация информационных угроз, обусловленных технологической зависимостью функционирования объектов информационной инфраструктуры кредитной организации от поставщиков услуг в сфере информационных технологий.

6.5. Кредитные организации в части тестирования операционной надежности технологических процессов должны принимать организационные и технические меры, направленные на проведение сценарного анализа (в части возможной реализации информационных угроз в отношении критичной архитектуры, а также возникновения сбоев объектов информационной инфраструктуры), с учетом требований

подпункта 2.1.5 пункта 2.1 Положения Банка России № 716-П и проводить с использованием результатов сценарного анализа тестирование готовности кредитной организации противостоять реализации информационных угроз в отношении критичной архитектуры.

6.6. Кредитные организации в части нейтрализации информационных угроз со стороны внутреннего нарушителя разрабатывают и принимают организационные и технические меры в отношении субъектов доступа, привлекаемых в рамках выполнения технологических процессов, направленные на исключение возможности несанкционированного использования предоставленных указанным субъектам доступа полномочий.

6.7. Кредитные организации должны обеспечивать выполнение следующих требований к обеспечению осведомленности об информационных угрозах:

организация взаимодействия кредитной организации и иных участников технологического процесса при обмене информацией об актуальных сценариях реализации информационных угроз;

использование информации об актуальных сценариях реализации информационных угроз в целях обеспечения непрерывного оказания банковских услуг.

7. Кредитные организации должны обеспечить нейтрализацию информационных угроз в отношении возникновения зависимости обеспечения операционной надежности от субъектов доступа, являющихся работниками кредитной организации, обладающими уникальными знаниями, опытом и компетенцией в области разработки технологических процессов, поддержания их выполнения, реализации технологических процессов, которые отсутствуют у иных работников указанной кредитной организации.

Кредитные организации должны обеспечить защиту критичной архитектуры от возможной реализации информационных угроз в условиях

дистанционной (удаленной) работы работников кредитной организации.

8. Кредитные организации, размер активов которых составляет 500 миллиардов рублей и более на начало текущего отчетного года в соответствии со значением статьи «Всего активов», определяемым в соответствии с Разработочной таблицей для составления бухгалтерского баланса (публикуемой формы) пункта 3 Порядка составления и представления отчетности по форме 0409806 «Бухгалтерский баланс (публикуемая форма)», установленного приложением 1 к Указанию Банка России от 8 октября 2018 года № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации»[8], и которые являются субъектами критической информационной инфраструктуры в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ, должны выполнять требования, направленные на противодействие целевым компьютерным атакам в зависимости от уровня опасности, установленные федеральным органом исполнительной власти, уполномоченным в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

9. Кредитные организации должны установить во внутренних документах, предусмотренных подпунктом 4.1.2, абзацем первым подпункта 4.1.3 и абзацем вторым подпункта 4.1.4 пункта 4.1 Положения Банка России № 716-П, описание процедур, направленных на реализацию требований к операционной надежности, включая:

определение и описание состава процедур, направленных на

---

[8] Зарегистрировано Минюстом России 13 декабря 2018 года, регистрационный № 52992, с изменениями, внесенными Указаниями Банка России от 20 ноября 2019 года № 5320-У (зарегистрировано Минюстом России 13 декабря 2019 года, регистрационный № 56796), от 12 мая 2020 года № 5456-У (зарегистрировано Минюстом России 18 июня 2020 года, регистрационный № 58705), от 10 августа 2020 года № 5526-У (зарегистрировано Минюстом России 30 сентября 2020 года, регистрационный № 60147), от 12 января 2021 года № 5705-У (зарегистрировано Минюстом России 15 апреля 2021 года, регистрационный № 63150), от 17 февраля 2021 года № 5736-У (зарегистрировано Минюстом России 26 марта 2021 года, регистрационный № 62892), от 20 апреля 2021 года № 5783-У (зарегистрировано Минюстом России 11 июня 2021 года, регистрационный № 63866), от 8 ноября 2021 года № 5986-У (зарегистрировано Минюстом России 14 декабря 2021 года, регистрационный № 66316).

выполнение требований к операционной надежности;

определение перечня и порядка организационного взаимодействия подразделений кредитной организации, участвующих в соблюдении требований к операционной надежности, с учетом исключения конфликта интересов;

определение порядка осуществления контроля за соблюдением требований к операционной надежности в рамках системы внутреннего контроля;

выделение ресурсного обеспечения для выполнения требований к операционной надежности;

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

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

10. Кредитные организации в рамках обеспечения операционной надежности должны:

моделировать информационные угрозы в отношении критичной архитектуры с учетом требований к проведению качественной оценки уровня операционного риска, предусмотренных подпунктом 2.1.5 пункта 2.1 Положения Банка России № 716-П;

планировать применение организационных и технических мер, направленных на реализацию требований к операционной надежности, с учетом результатов идентификации риска информационной безопасности, а также его оценки, проводимой в составе процедур управления операционным риском в соответствии с требованиями глав 2 и 7 Положения Банка России № 716-П;

обеспечивать реализацию требований к операционной надежности на стадиях создания, ввода в эксплуатацию, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации,

вывода из эксплуатации объектов информационной инфраструктуры;

обеспечивать контроль соблюдения требований к операционной надежности.

Кредитные организации должны включать в порядок ведения базы событий, предусмотренный пунктом 6.2 Положения Банка России № 716-П, особенности регистрации событий операционного риска, являющихся инцидентами операционной надежности.

Кредитная организация должна регистрировать инциденты операционной надежности с учетом требований к ведению базы событий, предусмотренных главой 6 Положения Банка России № 716-П.

Кредитные организации при определении в соответствии с пунктом 3.7 Положения Банка России № 716-П дополнительных типов событий операционного риска должны предусматривать во внутренних документах классификацию типов инцидентов операционной надежности с использованием перечня типов инцидентов операционной надежности, размещаемого Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), и обеспечивать их регулярную актуализацию.

По каждому инциденту операционной надежности в дополнение к информации, указанной в пункте 6.6 Положения Банка России № 716-П, кредитные организации должны обеспечить регистрацию следующей информации:

данных, используемых для фиксации превышения установленных значений целевых показателей операционной надежности;

данных, позволяющих выявить причину превышения установленных значений целевых показателей операционной надежности;

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

операционной надежности).

Кредитные организации должны устанавливать во внутренних документах критерии шкалы качественных оценок и методику определения оценок качественных потерь от реализации инцидентов операционной надежности в соответствии с подпунктом 3.13.2 пункта 3.13 Положения Банка России № 716-П, в случае если они не определяются в денежном выражении.

11. Кредитные организации в рамках обеспечения операционной надежности должны информировать Банк России:

о выявленных инцидентах операционной надежности (в случае превышения допустимой доли деградации технологических процессов), а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитной организацией или Банком России инцидент 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», в отношении указанных в абзаце втором настоящего пункта инцидентов операционной надежности не позднее одного рабочего дня до дня проведения мероприятия.

Кредитные организации должны представлять в Банк России указанные в абзацах втором и третьем настоящего пункта сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России), информация о которых размещается на официальном сайте Банка России в сети «Интернет».

12. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 23 декабря 2021 года № ПСД-32) вступает в силу с 1 октября 2022 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Положению Банка России от 12 января 2022 года № 787-П
«Об обязательных для кредитных организаций требованиях
к операционной надежности при осуществлении банковской
деятельности в целях обеспечения непрерывности оказания
банковских услуг»

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

№ п/п	Наименование технологического процесса	Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов (в часах)			
		для банка, размер активов которого составляет 500 миллиардов рублей и более	для банка с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей	для банка с базовой лицензией	для небанковской кредитной организации
1	2	3	4	5	6
1	Технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады	2	4	6	X
2	Технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады	2	4	6	6
3	Технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет	2	4	6	6

1	2	3	4	5	6
4	Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам	2	4 2 –для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России от 6 ноября 2014 года № 3439-У «О порядке признания Банком России кредитных организаций значимыми на рынке платежных услуг»[1] (далее – Указание Банка России № 3439-У)	6 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У	X
5	Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам, за исключением переводов по распоряжениям участников платежной системы (для переводов денежных средств по распоряжениям участников платежной системы – в соответствии с Положением Банка России от 3 октября 2017 года № 607-П	2	4 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У	6 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У	6 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У

[1] Зарегистрировано Минюстом России 3 декабря 2014 года, регистрационный № 35075, с изменениями, внесенными Указаниями Банка России от 27 октября 2016 года № 4170-У (зарегистрировано Минюстом России 16 ноября 2016 года, регистрационный № 44349), от 2 ноября 2017 года № 4597-У (зарегистрировано Минюстом России 27 ноября 2017 года, регистрационный № 49019).

1	2	3	4	5	6
	«О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков»[1])				
6	Технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц	2	2	2	X
7	Технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц	2	2	2	2
8	Технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)	2	4 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У	6 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У	6 2 – для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России № 3439-У
9	Технологический процесс, обеспечивающий выполнение операций на финансовых рынках	24	24	24	X
10	Технологический процесс, обеспечивающий выполнение кассовых операций	2	2	2	X

[1] Зарегистрировано Минюстом России 22 декабря 2017 года, регистрационный № 49386.

1	2	3	4	5	6
11	Технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	2	2	2	X
12	Технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе	2	2	2	X
13	Технологический процесс, обеспечивающий идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия	2	2	2	X