

**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)**

П О Л О Ж Е Н И Е

«___» _____ 202_ г.

№ _____ -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 57⁵ Федерального закона Российской Федерации 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) устанавливает обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг.

1. Кредитные организации должны выполнять 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», зарегистрированным Министерством юстиции Российской Федерации 3 июня 2020 года № 58577 (далее – Положение Банка России № 716-П), при осуществлении банковской деятельности с использованием информационных систем для целей

обеспечения непрерывности функционирования критически важных процессов, определяемых кредитной организацией с учетом подпункта 4.1.1 пункта 4.1 Положения Банка России № 716-П.

Под операционной надежностью в настоящем Положении понимается способность кредитной организации обеспечить непрерывность функционирования критически важных процессов с учетом соблюдения контрольных показателей уровня операционного риска для целей обеспечения операционной надежности, устанавливаемых кредитной организацией в соответствии с пунктом 3 настоящего Положения, в случае возникновения отказов и (или) нарушений функционирования применяемых кредитной организацией информационных, технологических и других систем, оборудования и (или) несоответствия их функциональных возможностей и характеристик потребностям кредитной организации и (или) реализации киберриска в значении, установленном в пункте 7.2 Положения Банка России № 716-П.

2. Кредитные организации должны обеспечить непревышение порогового уровня допустимого времени простоя технологических процессов, обеспечивающих выполнение критически важных процессов, определяемых кредитной организацией с учетом подпункта 4.1.1 пункта 4.1 Положения Банка России № 716-П, и указанных в приложении к настоящему Положению, и (или) нарушения технологических процессов, обеспечивающих выполнение критически важных процессов, приводящего к неоказанию или ненадлежащему оказанию банковских услуг (далее – деградация технологических процессов), в соответствии с 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 контрольные показатели уровня операционного риска для целей обеспечения операционной

надежности (далее – целевые показатели 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 банковских услуг (в случае превышения допустимой доли деградации технологических процессов) (далее – инцидент операционной надежности) к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания банковских услуг, рассчитанное кредитной организацией с учетом статистических данных за период не менее двенадцати календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности, и (или) экспертного мнения (далее – допустимая доля деградации технологических процессов);

допустимого времени простоя и (или) деградации технологического процесса в рамках инцидента операционной надежности (в случае превышения 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 (времени начала, времени окончания, продолжительности и последовательности технологических процессов).

В случае, если технологический процесс функционирует менее двенадцати календарных месяцев, то кредитные организации должны определять целевые показатели операционной надежности с учетом статистических данных за период с даты начала его функционирования.

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, 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 проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов.

4. Кредитные организации с учетом требований главы 5 Положения Банка России № 716-П должны определить сигнальные и контрольные значения целевых показателей операционной надежности.

Кредитная организация должна 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.

5. Кредитные организации разрабатывают во внутренних документах и выполняют требования к операционной надежности, которые включают в себя:

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

требования в отношении идентификации состава элементов, указанных в подпункте 5.1 настоящего пункта Положения (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 с учетом требований к выявлению событий риска информационной безопасности порядку реагирования на выявленные события риска информационной безопасности и восстановления деятельности кредитной организации в случае реализации таких событий, устанавливаемых главой 7 Положения Банка России № 716-П;

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

требования в отношении тестирования операционной надежности технологических процессов;

требования в отношении нейтрализации угроз со стороны несанкционированного доступа работников кредитной организации или

работников поставщиков услуг в сфере информационных технологий, обладающих полномочиями доступа к программно-аппаратным средствам (далее – внутренний нарушитель), к программно-аппаратным средствам;

требования в отношении обеспечения осведомленности кредитной организации об актуальных информационных угрозах;

иные требования, установленные пунктами 6-11 настоящего Положения.

5.1. Кредитные организации в отношении идентификации критичной архитектуры должны обеспечивать организацию учета и контроля состава следующих элементов критичной архитектуры:

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);

информационных систем, программно-аппаратных средств кредитной организации, задействованных при выполнении каждого технологического процесса;

технологических участков (этапов) технологических процессов, установленных в пункте 5.2 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», зарегистрированного Министерством юстиции Российской Федерации 16 мая 2019 года № 54637 (далее соответственно – Положение Банка России № 683-П, технологические участки (этапы) технологических процессов);

технологических процессов, технологических участков (этапов) 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 программно-аппаратным средствам (далее – субъекты доступа), задействованных при выполнении каждого технологического процесса;

взаимосвязей и взаимозависимостей между кредитными организациями и 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 пункте 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 (этапов) технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий, кредитные организации должны обеспечивать ведение соответствующего реестра в соответствии с внутренними документами.

5.2. Кредитные организации 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 превышение (отклонение от) значений целевых показателей операционной надежности;

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

управление конфигурациями (настраиваемыми параметрами)
программно-аппаратных средств;

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

5.3. Кредитные 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, включая 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 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 программно-аппаратных средств после реализации инцидентов операционной надежности.

5.4. Кредитные организации должны обеспечивать выполнение следующих требований в отношении взаимодействия с поставщиками услуг в сфере информационных технологий:

нейтрализацию информационных угроз при привлечении поставщиков услуг в сфере информационных технологий, в том числе защиту программно-аппаратных средств от возможной реализации информационных угроз со стороны поставщиков услуг в сфере информационных технологий;

нейтрализацию информационных угроз, обусловленных технологической зависимостью функционирования программно-аппаратных средств кредитной организации от поставщиков услуг в сфере информационных технологий.

5.5. Кредитные организации в отношении тестирования операционной надежности технологических процессов должны принимать организационные и технические меры, направленные на проведение сценарного анализа (в части возможной реализации информационных угроз) с учетом требований подпункта 2.1.5 пункта 2.1 Положения Банка России № 716-П, и тестирования с использованием его результатов готовности кредитной организации противостоять реализации информационных угроз в отношении критичной архитектуры.

5.6. Кредитные организации в отношении нейтрализации 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.

5.7. Кредитные организации должны обеспечивать выполнение следующих требований в отношении обеспечения осведомленности об актуальных информационных угрозах:

организацию 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 для цели обеспечения непрерывного оказания банковских услуг.

6. Кредитные организации должны обеспечить нейтрализацию угроз в отношении возникновения зависимости обеспечения операционной надежности от субъектов доступа – работников кредитной организации, обладающих уникальными знаниями, опытом и компетенцией.

Кредитная организация должна обеспечить защиту критичной архитектуры от возможной реализации информационных угроз при условии дистанционной работы работников кредитной организации.

7. В целях организации реагирования на угрозы проведения целевых компьютерных атак по требованию Банка России банки, размер активов которых составляет 500 миллиардов рублей и более, в значении, установленном в пункте 9.1 Положения Банка России № 716-П, должны выполнять настоящее Положение с учетом:

реализации мер противодействия целевым компьютерным атакам;

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

внеплановой оценки защищенности критичной архитектуры и устранение выявленных недостатков;

оперативного взаимодействия службы информационной безопасности в значении, установленном в пункте 7.5 Положения Банка России № 716-П, функционирующей в оперативном режиме работы, с Банком России.

Кредитные организации определяют во внутренних документах порядок оперативного взаимодействия подразделений, обеспечивающих выполнение технологических процессов, со службой информационной безопасности для целей настоящего Положения.

8. Кредитные организации устанавливают во внутренних документах, включаемых в состав внутренних документов по управлению

операционным риском, указанных в подпунктах 4.1.2–4.1.4 пункта 4.1 Положения Банка России № 716-П, описание процедур, направленных на реализацию требований к операционной надежности, установленных настоящим Положением, включая:

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

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

определение во внутренних документах порядка осуществления и соблюдение контроля за соблюдением требований настоящего Положения 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.

9. В целях реализации требований к операционной надежности кредитная организация должна:

моделировать информационные угрозы в отношении критичной архитектуры с учетом требований к проведению качественной оценки операционных рисков с учетом подпункта 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 с учетом глав 2 и 7 Положения Банка России № 716-П;

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

обеспечивать контроль соблюдения требований настоящего Положения.

Кредитные организации включают в порядок ведения базы событий, указанный в пункте 6.2 Положения Банка России № 716-П, особенности регистрации событий операционного риска, являющихся инцидентами операционной надежности.

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

Кредитные организации определяют во внутренних документах с учетом пункта 3.7 Положения Банка России № 716-П дополнительную классификацию типов инцидентов операционной надежности, соответствующую перечню типов инцидентов операционной надежности, размещаемому Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), и обеспечивают их регулярную актуализацию с данным перечнем.

По каждому инциденту операционной надежности в дополнение к информации, указанной в пункте 6.6 Положения Банка России № 716-П, кредитные организации определяют дополнительные поля для регистрации следующей информации:

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 кредитной организацией или Банком России инцидент операционной надежности).

Кредитные организации устанавливают во внутренних документах критерии шкалы качественных оценок и методику определения оценок для качественных потерь от реализации инцидентов операционной надежности согласно абзацу одиннадцатому подпункта 3.13.2 пункта 3.13 Положения Банка России № 716-П..

10. Кредитные 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 сети «Интернет», а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитной 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.

Кредитные организации должны предоставлять в Банк России указанные в абзацах втором и третьем настоящего пункта Положения сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия кредитных организаций с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России кредитные 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».

11. Кредитные организации должны выполнять требования настоящего Положения с учетом требований главы 9 Положения Банка России № 716-П.

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

Председатель
Центрального банка
Российской Федерации

Э.С. Набиуллина

Приложение
к Положению Банка России от
___ №___ «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**

Приложение к настоящему Положению в зависимости от характера и масштаба деятельности применяют следующие кредитные организации:

банк, размер активов которого составляет 500 миллиардов рублей и более, в значении, установленном в пункте 9.1 Положения Банка России № 716-П;

банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, в значении, установленном в пункте 9.2 Положения Банка России № 716-П;

банк с базовой лицензией в значении, установленном в пункте 9.3 Положения Банка России № 716-П;

небанковская кредитная организация в значении, установленном в пункте 9.4 Положения Банка России № 716-П.

№	Наименование технологического процесса	Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов			
		Банк, размер активов которого составляет 500 миллиардов рублей и более,	Банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей,	Банк с базовой лицензией	Небанковская кредитная организация

1	2	3	4	5	6
1	Технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады	2 ч.	2 ч.	2 ч.	X
2	Технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады	2 ч.	2 ч.	2 ч.	2 ч.
3	Технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет	2 ч.	2 ч.	2 ч.	2 ч.
4	Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам	2 ч.	2 ч.	2 ч.	2 ч.
5	Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам	2 ч.	2 ч.	2 ч.	2 ч.
6	Технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц	2 ч.	2 ч.	2 ч.	X
7	Технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц	2 ч.	2 ч.	2 ч.	2 ч.
8	Технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)	2 ч.	2 ч.	2 ч.	2 ч.
9	Технологический процесс, обеспечивающий выполнение операций на финансовых рынках	24 ч.	24 ч.	24 ч.	X
10	Технологический процесс, обеспечивающий выполнение кассовых операций	2 ч.	2 ч.	2 ч.	X
11	Технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	2 ч.	2 ч.	2 ч.	X
12	Технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе	0,5 ч	2 ч.	2 ч.	X
13	Технологический процесс, обеспечивающий идентификацию и	2 ч.	2 ч.	2 ч.	X

	(или) аутентификацию с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия.				
--	--	--	--	--	--