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

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел.: (499) 300-30-00, 8 (800) 300-30-00

Личный кабинет

Вице-президенту
Ассоциации банков России

А.А. Войлукову

ИНН 7702077663

От 06.10.2021 № 56-15/998

на 02-05/894 от 07.09.2021

О рассмотрении обращения

Уважаемый Алексей Арнольдович!

Департамент информационной безопасности рассмотрел замечания, предложения и вопросы кредитных организаций – членов Ассоциации банков России по проекту положения Банка России «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» (далее – Проект положения) и по существу поступивших вопросов сообщает следующее.

По вопросу, содержащемуся в пункте 1

Указанные в приложении технологические процессы императивно установлены и не могут носить характер рекомендательных. Вместе с тем кредитная организация может самостоятельно дополнить указанный перечень с учетом своей системы управления операционными рисками. В приложении 5 к Положению Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» (далее – Положение Банка России № 242-П) не указаны конкретные критически важные процессы. Вместе с тем при выполнении требований Положения Банка России № 242-П в рамках плана ОНиВД допустимо формировать перечень критически важных процессов, совпадающий с перечнем технологических процессов, указанных в приложении к Проекту положения.

Требования к определению перечня критически важных процессов установлены в Положении Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (далее – Положение Банка Росси № 716-П).

По вопросу, содержащемуся в пункте 2

Термин используется в значении, указанном в Положении Банка России № 716-П, и включает, например, автоматизированные системы.

По вопросу, содержащемуся в пункте 3

Определение технологического процесса планируется ввести указанием Банка России «О внесении изменений в Положение Банка России № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

По вопросу, содержащемуся в пункте 4

Верное понимание. Пороговый уровень относится не только к простою (100%-ная деградация), но и к деградации технологических процессов, которая приводит к неоказанию или ненадлежащему оказанию банковских услуг.

По вопросу, содержащемуся в пункте 5

Допустимая доля деградации технологических процессов устанавливается на усмотрение кредитной организации, соответствующее уточнение добавлено в Проект положения. Простой является случаем 100%-ной деградации.

По вопросу, содержащемуся в пункте 7

Контрольные показатели уровня операционного риска для целей обеспечения операционной надежности (целевые показатели операционной надежности) входят в систему контрольных показателей уровня операционного риска, требования к которой установлены главой 5 Положения Банка России № 716-П. Установление целевых показателей операционной надежности вне приложения 1 к Положению Банка России № 716-П обусловлено целесообразностью отражения ключевых требований к операционной надежности в рамках одного нормативного акта.

По вопросу, содержащемуся в пункте 10

Случаи, связанные с неоказанием или ненадлежащим оказанием кредитной организацией услуг в результате простоя и (или) деградации технологических процессов по не зависящим от нее обстоятельствам, необходимо признавать инцидентами операционной надежности.

Проведение плановых технологических операций не относится к инцидентам операционной надежности. В Проекте положения содержится указание, что при определении времени простоя и (или) деградации

технологических процессов в расчет не включаются установленные во внутренних документах периоды времени проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов.

По вопросу, содержащемуся в пункте 11

Кредитная организация вправе принимать соответствующие решения по установлению дополнительных целевых показателей операционной надежности. Модификация императивно установленных Проектом положения целевых показателей операционной надежности не допускается.

По вопросу, содержащемуся в пункте 12

В Проекте положения не установлено требование о необходимости непрерывного режима работы всех технологических процессов.

Согласно Проекту положения кредитной организации необходимо установить во внутренних документах для каждого технологического процесса (определенных в приложении к Проекту положения) значения целевого показателя операционной надежности: «показателя соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса)». Таким образом, операционная надежность технологических процессов рассматривается только относительно установленного режима работы.

Также в проекте содержится указание, что при определении времени простоя и (или) деградации технологических процессов в расчет не включаются установленные во внутренних документах периоды времени проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов.

По вопросу, содержащемуся в пункте 13

Проектом положения установлено, что 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).

По вопросу, содержащемуся в пункте 14

Способ фиксации указанных данных кредитные организации определяют самостоятельно. При этом следует обеспечить фиксацию фактических значений. Полагаем возможной фиксацию таких данных при

регистрации инцидентов операционной надежности в базе событий операционной надежности справочно дополнительными полями.

При этом обращаем внимание, что фактическое время простоя и (или) деградации технологического процесса исчисляется по каждому инциденту операционной надежности, в то время как суммарное время простоя и (или) деградации технологического процесса определяется за 12 месяцев, что должно учитываться при выборе способа фиксации указанных данных.

По вопросу, содержащемуся в пункте 15

В случае превышения планового временного периода проведения технологических операций кредитные организации обязаны учитывать превышение запланированного периода при определении времени простоя и (или) деградации технологических процессов.

По вопросу, содержащемуся в пункте 17

Расчет сигнальных и контрольных значений контрольных показателей уровня операционного риска в части операционной надежности кредитные организации осуществляют самостоятельно (для показателя «допустимое время простоя и (или) деградации технологического процесса» должен быть учтен пороговый уровень, установленный в приложении к Проекту положения). Проведение анализа необходимости пересмотра осуществляется в целях фиксации решения относительно необходимости или отсутствия необходимости изменения значений целевых показателей операционной надежности.

По вопросу, содержащемуся в пункте 18

Требования к операционной надежности устанавливаются настоящим Проектом положения в целом. Пункт 3 настоящего Проекта положения и глава 5 Положения Банка России № 716-П устанавливают требования к контрольным показателям уровня операционного риска для целей обеспечения операционной надежности (целевым показателям операционной надежности). Кредитная организация вправе разработать дополнительные (к установленным императивно) целевые показатели операционной надежности.

По вопросу, содержащемуся в пункте 23

В случае если сбой у внешнего поставщика привел к простою и (или) деградации технологического процесса кредитной организации, информирование необходимо; о сбоях у банков-контрагентов информирование не требуется.

По вопросу, содержащемуся в пункте 25

В части требований к нейтрализации угроз в отношении возникновения зависимости обеспечения операционной надежности от субъектов доступа –

работников кредитной организации, обладающих уникальными знаниями, опытом и компетенцией, понимание верное.

В части требований к нейтрализации реализации информационных угроз при удаленной (дистанционной) работе, в первую очередь, предполагается реализация мер, направленных на реализацию процесса «защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств», определенных ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее – ГОСТ Р 57580.1-2017). Полагаем, что в качестве признаков/показателей, по которым можно оценить возможность реализации информационных угроз при удаленной (дистанционной) работе, могут, как минимум, выступать показатели, характеризующие полноту и качество применяемых мер, направленных на реализацию процесса «защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств», определенных ГОСТ Р 57580.1-2017.

По вопросу, содержащемуся в пункте 26

За основу был взят критерий, характеризующий масштабы деятельности и значимость кредитной организации. Подход по установлению требований именно в отношении банков определен аналогично применяемому в рамках Положения Банка России № 716-П подходу, имеющему ограниченное распространение требований на небанковские кредитные организации. Требования настоящего пункта связаны с необходимостью обеспечения готовности кредитных организаций, масштабы деятельности которых оказывают значимое влияние на функционирование финансовой системы, к возможным целевым компьютерным атакам и направлены именно на указанные кредитные организации.

По вопросу, содержащемуся в пункте 27

Предполагается, что в случае выявления такой необходимости по требованию Банка России должны будут проводиться плановые тренировки (учения) по проверке готовности к действиям в отношении определенных целевых компьютерных атак, которые могут быть интегрированы кредитной организацией в процесс тестирования готовности противостоять реализации информационных угроз в отношении критичной архитектуры. Предполагается, что плановые тренировки (учения) по проверке готовности к действиям в отношении определенных целевых компьютерных атак будут более узконаправленными.

По вопросу, содержащемуся в пункте 28

Моделирование сценариев целевых компьютерных атак проводится по требованию Банка России и является более узконаправленным мероприятием (в отношении определенных целевых компьютерных атак) в отличие от моделирования информационных угроз. Предполагается, что данные мероприятия будут интегрированы в сценарный анализ, требования к проведению которого установлены Положением Банка России № 716-П.

Также норму относительно проведения моделирования угроз предполагается установить указанием Банка России «О внесении изменений в Положение Банка России № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

Под уровнем опасности понимаются особые условия, при которых возможна реализация целевых компьютерных атак в отношении кредитных организаций. Под внеплановой оценкой защищенности критичной архитектуры понимается проведение внепланового тестирования готовности противостоять определенным целевым компьютерным атакам (целевой компьютерной атаке).

По вопросу, содержащемуся в пункте 31

Определение необходимости отражения положений пункта 8 Проекта положения в рамках Политики управления операционным риском остается на усмотрение кредитной организации. При этом полагаем необходимым отражение положений указанного пункта Проекта положения в рамках остальных документов, определенных пунктами 4.1.2 – 4.1.4 Положения Банка России № 716-П.

По вопросу, содержащемуся в пункте 32

Предполагается, что кредитная организация самостоятельно определяет подход к осуществлению контроля за соблюдением требований к обеспечению операционной надежности, устанавливаемых Проектом положения, в рамках системы внутреннего контроля кредитной организации.

По вопросам, содержащимся в пунктах 35, 41, 43

По аналогии с инцидентами защиты информации сведения об инцидентах операционной надежности необходимо будет представлять в соответствии со стандартом Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации», который будет доработан в части инцидентов операционной надежности и размещен на сайте Банка России, в разделе «Информационная безопасность»,

«Стандарты Банка России». Ссылка на ненормативный акт недопустима по требованиям Минюста России. В этой связи дана ссылка на официальный сайт Банка России, указание конкретной веб-ссылки недопустимо. Во внутренних документах можно будет сделать отсылку на СТО БР БФБО-1.5-2018 (после его доработки в обновленном виде с учетом инцидентов операционной надежности).

Канал взаимодействия – уже используемый по инцидентам защиты информации – АСОИ ФинЦЕРТ.

Информирование об отсутствии инцидентов операционной надежности не требуется.

По вопросу, содержащемуся в пункте 36

Кредитная организация самостоятельно определяет объем и содержание указанной информации. Необходимо зафиксировать те данные (в частности, технические), которые позволят сделать вывод о причине возникновения инцидента операционной надежности, а также данные, указывающие на превышение целевых показателей операционной надежности.

По вопросу, содержащемуся в пункте 38

С учетом требований главы 9 Положения Банка России № 716-П данное требование не распространяется на кредитные организации с размером активов менее 500 млрд рублей.

По вопросу, содержащемуся в пункте 42

В Проекте положения указано, что все требования к операционной надежности должны учитываться на всем жизненном цикле программно-аппаратных средств. Предполагается, что требования должны закладываться на стадии создания, чтобы обеспечить соответствие вводимых в эксплуатацию программно-аппаратных средств, а также учитывать влияние вывода из эксплуатации (в том числе с обеспечением корректного выведения из эксплуатации) программно-аппаратных средств на операционную надежность.

По вопросу, содержащемуся в пункте 45

В соответствии с Гражданским кодексом Российской Федерации индивидуальным предпринимателем является физическое лицо, занимающееся предпринимательской деятельностью без образования юридического лица, а товарищество может быть как с образованием юридического лица, так и без.

По вопросу, содержащемуся в пункте 46

Пороговые уровни увеличены для некрупных кредитных организаций. Понятие «рабочие часы» отсутствует в законодательстве Российской Федерации. Имеются в виду «календарные» часы. Возможность учета плановых перерывов в осуществлении технологических процессов (регламентное время работы технологических процессов – рабочее / нерабочее время, а также проведение плановых технологических операций) предусмотрена в Проекте положения. Санкции за невыполнение установлены в статье 74 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)». Требования по срокам будут установлены в соответствии с нормативным актом. В случае обстоятельств непреодолимой силы невыполнение требований не повлечет санкции. Банк России готовит информационные письма о неприменении мер в случае таких ситуаций (например, в период пандемии новой коронавирусной инфекции Банк России опубликовал информационное письмо о неприменении мер надзорного реагирования по требованиям к защите информации). Информация о сбоях необходима Банку России для выполнения его функций по обеспечению стабильности банковской системы и защиты интересов вкладчиков и кредиторов. Так, информация о допущенных сбоях, произошедших ввиду компьютерных атак, будет доведена до сведения иных кредитных организаций для предотвращения подобных сбоев.

По вопросу, содержащемуся в пункте 47

Определение инцидента операционной надежности, приведенное в Проекте положения, подразумевает событие операционного риска или серию связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к неоказанию или ненадлежащему оказанию банковских услуг. Таким образом, серия связанных событий должна рассматриваться как один инцидент операционной надежности.

По вопросу, содержащемуся в пункте 48

Значения порогового уровня установлены с учетом значимости непревышения указанных целевых значений в отношении технологических процессов (приведенных в приложении к Проекту положения) с точки зрения интересов как потребителей банковских услуг, так и кредитных организаций.

Под пороговым временем для операций на финансовых рынках понимается предельно допустимое время простоя и (или) деградации технологического процесса на стороне кредитной организации. Пороговое значение для технологических процессов биржи установлено в нормативном

акте о требованиях к операционной надежности для некредитных финансовых организаций и составляет 2 часа.

В части технологических процессов, связанных со взаимодействием с единой биометрической системой, пороговое значение увеличено до 2 часов.

По вопросу, содержащемуся в пункте 49

Согласно Проекту положения кредитной организации необходимо будет установить во внутренних документах для каждого технологического процесса (определенных в приложении к Проекту положения) значения целевого показателя операционной надежности: «показателя соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса)». Таким образом, операционная надежность технологических процессов рассматривается только относительно установленного режима работы.

Также в Проекте положения содержится указание, что при определении времени простоя и (или) деградации технологических процессов в расчет не включаются установленные во внутренних документах периоды времени проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) технологических процессов.

По вопросу, содержащемуся в пункте 56

Расчет фактической доли деградации технологического процесса должен проводиться исходя из фактического и ожидаемого количества финансовых операций. Определение ожидаемого количества финансовых операций должно осуществляться организацией с учетом статистических данных и (или) иных данных по выбору кредитной организации.

По вопросу, содержащемуся в пункте 61

Согласно Проекту положения к инцидентам операционной надежности относятся случаи простоя и (или) деградации технологических процессов как в результате реализации операционного риска, обусловленного источниками риска, относящимися к категории «сбои систем и оборудования», так и в результате реализации киберриска.

По вопросу, содержащемуся в пункте 63

Для банков с универсальной лицензией регистрация инцидентов операционной надежности в базе событий операционного риска будет обязательной в случае возникновения прямых потерь и (или) косвенных потерь, и (или) потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 Положения Банка России № 716-П.

Для банков с базовой лицензией регистрация инцидентов операционной надежности в базе событий операционного риска будет обязательной в случае возникновения прямых потерь и (или) потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 Положения Банка России № 716-П.

Директор Департамента
информационной безопасности В.А. Уваров