



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

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

От 01.11.2022 № 56-27/1367

на № 82 от 04.10.2022

О рассмотрении обращения

Личный кабинет

АНО «Центр ИксБиАрЭл»

ИНН 9710043968

Банк России рассмотрел обращение Автономной некоммерческой организации «Центр по внедрению и развитию формата ИксБиАрЭл» (АНО «Центр ИксБиАрЭл») Положения Банка России от 15.11.2022 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований 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)» (далее – Положение Банка России № 779-П) и сообщает следующее.

По вопросу 1. Целевой показатель операционной надежности допустимое время простоя и (или) деградации технологического процесса в рамках события операционного риска, связанного с нарушением операционной надежности (в случае превышения допустимой доли деградации технологического процесса), устанавливается некредитными финансовыми организациями не выше порогового уровня, установленного в приложении к Положению Банка России № 779-П.

Целевой показатель операционной надежности допустимого суммарного времени простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу каждого календарного месяца устанавливается некредитной финансовой организацией самостоятельно.

Для расчета пороговых значений некредитные финансовые организации вправе применять собственные методики, обосновывающие сделанный выбор. При этом рекомендуем применять подход предусматривающий использование статистических данных за предыдущие аналогичные периоды. В случае отсутствия статистических данных может использоваться экспертный метод.

По вопросу 2. Некредитные финансовые организации самостоятельно определяют формат реализации требования к организации учета и контроля состава элементов критичной архитектуры.

Рекомендуется обеспечить автоматизацию соответствующего процесса в некредитной финансовой организации, в целях поддержания в актуальном состоянии информацию об элементах критичной архитектуры. Вместе с тем допускается ведение учета и контроля состава элементов критичной архитектуры неавтоматизированным способом.

По вопросу 3. В качестве мероприятий, направленных на снижение риска возникновения зависимости обеспечения операционной надежности от субъектов доступа – работников, обладающих знаниями, опытом и компетенцией, которые отсутствуют у всех иных работников (далее – ключевые работники), могут рассматриваться:

регламентация основных действий в рамках выполнения ключевыми работниками своих функций, оказывающих влияние на операционную надежность;

планирование привлечения внешней экспертизы для выполнения функций, осуществляемых ключевыми работниками;

организация мероприятий, направленных на обмен опытом ключевых работников с иными работниками некредитной финансовой организации, обладающих схожими компетенциями.

По вопросу 4. Указанное требование применяется некредитными финансовыми организациями в случае организации ими удаленной работы для субъектов доступа, входящих в критичную архитектуру.

По вопросу 5. Необходимо учитывать те взаимосвязи и взаимозависимости с иными организациями, от которых зависит операционная надежность технологических процессов. Данная информация потребуется при представлении финансовыми организациями информации о поставщиках услуг в рамках форм отчетности по операционной надежности, планируемых к утверждению и сбору в 2023 году.

По вопросу 6. В соответствии с пунктом 1.10 Положения Банка России от 15.11.2021 № 779-П финансовым организациям необходимо предоставлять иным участникам технологического процесса информацию о сценариях реализации информационных угроз, актуальных для данных участников, реализация которых может привести к нарушению непрерывного оказания услуг в рамках технологического процесса. Канал взаимодействия определяется финансовой организацией самостоятельно.

Вместе с тем данное требование не устанавливает обязанность предоставлять иным участникам технологического процесса информацию об инцидентах информационной безопасности, произошедших в финансовой организации. В рамках обмена информацией о сценариях реализации информационных угроз финансовая организация самостоятельно определяет возможность раскрытия, а также объем и формат раскрываемой информации.

И.о. директора
Департамента информационной безопасности

А.О. Выборнов