

Пояснительная записка к проекту положения Банка России «Об установлении требований к операционной надежности при совершении финансовых сделок с использованием финансовой платформы» (далее - проект Положения)

Банк России разработал проект Положения для установления требований к операционной надежности при совершении финансовых сделок с использованием финансовой платформы.

Проект разработан на основе имеющего международного опыта. Так, ведущие международные организации, определяющие стандарты в области финансовой деятельности, такие как Комитет по платежам и рыночным инфраструктурам, Международная организация комиссий по ценным бумагам, Базельский комитет по банковскому надзору Банка международных расчетов и др., сформировали пакет международных документов, направленных на обеспечение операционной надежности (киберустойчивости) финансовых организаций. В проекте содержатся положения, аналогичные следующим документам указанных международных организаций: Guidance on cyber resilience for financial market infrastructures, Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions; BIS Working Papers No 840. Operational and cyber risks in the financial sector, Bank for International Settlements; Operational Resilience Principles: Consultative document, Note from the Operational Resilience Group, Basel Committee on Banking Supervision, Bank for International Settlements.

Проект Положения устанавливает:

требования по определению и обеспечению контроля значений показателей операционной надежности (допустимого времени простоя и (или) деградации технологических процессов, допустимого времени простоя и (или) деградации в рамках отдельного инцидента, доли деградации в рамках отдельного инцидента, установленного режима осуществления финансовых сделок с использованием финансовой платформы и др.);

требования в рамках процессов обеспечения операционной надежности

(идентификация критичной архитектуры, управление изменениями, управление конфигурациями и уязвимостями, выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации, взаимодействие с поставщиками услуг, планирование непрерывности деятельности и тестирование операционной надежности технологических процессов, управление риском внутреннего нарушителя, обеспечение ситуационной осведомленности об актуальных информационных угрозах);

требования к описанию деятельности в целях реализации процессов обеспечения операционной надежности;

требования к информированию Банка России о выявленных инцидентах операционной надежности.

Ответственные за получение экспертных заключений – Краева Ольга Сергеевна, заместитель начальника Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности (kraevaos@cbr.ru), Никитина Виктория Леонидовна, начальник отдела нормативного регулирования Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности (nikitinavl@cbr.ru).

Дата начала приема экспертных заключений – 23.11.2020.

Дата окончания приема экспертных заключений – 06.12.2020.