ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

«23» декабря 2020 г. № 5673-У

г. Москва

О требованиях к операционной надежности при совершении финансовых сделок с использованием финансовой платформы

Настоящее Указание на основании части 1 статьи 12 Федерального закона от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (Собрание законодательства Российской Федерации, 2020, № 30, ст. 4737) устанавливает требования к операционной надежности при совершении финансовых сделок с использованием финансовой платформы.

1. Операторы финансовой платформы должны выполнять требования к операционной надежности при совершении финансовых сделок с использованием финансовой платформы в целях обеспечения бесперебойного функционирования программно-аппаратных средств, предназначенных для осуществления деятельности оператора финансовой платформы и указанных в абзаце шестом подпункта 5.1 пункта 5 настоящего Указания (далее – программно-аппаратные средства).

2. Операторы финансовой платформы, реализующие стандартный уровень защиты информации в соответствии с требованиями, установленными

Банком России на основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2018, № 27, ст. 3950), должны обеспечить пороговый уровень допустимого времени простоя обеспечивающих совершение финансовых сделок с использованием финансовой платформы технологических процессов (далее – технологические процессы) и (или) нарушения технологических процессов, приводящего к неоказанию или ненадлежащему оказанию услуг, связанных с обеспечением возможности совершения финансовых сделок между потребителями финансовых услуг и финансовыми организациями или эмитентами с использованием финансовых платформ (далее – деградация технологических процессов), не более двух часов подряд.

Операторы финансовой платформы, не указанные в абзаце первом настоящего пункта, должны обеспечить пороговый уровень допустимого времени простоя и (или) деградации технологических процессов не более четырех часов подряд.

3. Операторы финансовой платформы должны определить во внутренних документах значения целевых показателей операционной надежности:

допустимого времени простоя и (или) деградации технологических процессов с учетом порогового уровня, установленного в пункте 2 настоящего Указания;

суммарного времени простоя и (или) деградации технологических процессов в течение календарного месяца;

допустимого отношения общего количества финансовых сделок, заключенных во время деградации технологических процессов в рамках события или серии связанных событий, вызванных информационными угрозами, которые привели или могли привести к нарушению бесперебойного функционирования программно-аппаратных средств (далее – инцидент

операционной надежности), в случае превышения допустимого времени простоя и (или) деградации технологических процессов, к ожидаемому количеству финансовых сделок за тот же период в случае бесперебойного функционирования программно-аппаратных средств, рассчитанное на основе статистических данных за период не менее одного года (далее – допустимая доля деградации технологических процессов);

показателя соблюдения режима работы (функционирования) финансовой платформы (времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых на финансовой платформе с целью обеспечения возможности совершения финансовых сделок).

В случаях превышения допустимого времени простоя и (или) деградации технологических процессов, а также отклонения от допустимой доли деградации технологических процессов операторы финансовой платформы должны обеспечить фиксацию:

фактического времени простоя и (или) деградации технологических процессов, исчисляемого по каждому инциденту операционной надежности;

фактической доли деградации технологических процессов в рамках отдельного инцидента операционной надежности.

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. Определение целевых показателей операционной надежности и обеспечение контроля за их соблюдением реализуется оператором финансовой платформы в рамках системы управления рисками.

Оператор финансовой платформы должен не реже одного раза в год проводить анализ необходимости пересмотра значений целевых показателей операционной надежности.

5. Требования к операционной надежности при совершении финансовых сделок с использованием финансовой платформы включают в себя:

требования к определению целевых показателей и обеспечению контроля за их соблюдением;

требования к операционной надежности в отношении идентификации состава элементов, указанных в подпункте 5.1 настоящего пункта (далее – критичная архитектура);

требования к операционной надежности в отношении управления изменениями критичной архитектуры;

требования к операционной надежности в отношении выявления, регистрации, реагирования на инциденты операционной надежности и восстановление выполнения технологических процессов и функционирования программно-аппаратных средств после реализации таких инцидентов;

требования к операционной надежности в отношении взаимодействия с внешними контрагентами, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов (далее – поставщики услуг);

требования к операционной надежности в отношении тестирования операционной надежности технологических процессов;

требования к операционной надежности в отношении управления риском несанкционированного доступа работников оператора финансовой платформы или работников поставщиков услуг, обладающих полномочиями доступа к программно-аппаратным средствам (далее – внутренний нарушитель);

требования к операционной надежности в отношении обеспечения осведомленности об актуальных информационных угрозах;

иные требования в соответствии с пунктами 6–9 настоящего Указания.

5.1. Операторы финансовой платформы в отношении идентификации

критичной архитектуры должны обеспечивать организацию учета и мониторинга следующих элементов критичной архитектуры:

технологических процессов, реализуемых непосредственно оператором финансовой платформы;

технологических процессов, реализуемых поставщиками услуг;

подразделений оператора финансовой платформы, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов (далее – подразделения оператора финансовой платформы);

технологических участков (этапов) технологических процессов;

программно-аппаратных средств оператора финансовой платформы, задействованных при выполнении каждого технологического процесса;

работников оператора финансовой платформы 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 оператором финансовой платформы, участниками финансовой платформы, регистратором финансовых транзакций, а также поставщиками услуг в рамках выполнения технологических процессов (далее при совместном упоминании – участники технологического процесса), в том числе взаимосвязей и взаимозависимостей между их программно-аппаратными средствами;

программно-аппаратных средств поставщиков услуг, задействованных при выполнении технологических процессов;

каналов передачи информации, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса при взаимодействии с работниками оператора финансовой платформы.

5.2. Операторы финансовой платформы должны обеспечивать

выполнение следующих требований к операционной надежности в отношении управления изменениями критичной архитектуры:

предотвращение возникновения уязвимостей 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 бесперебойного функционирования программно-аппаратных средств;

управление конфигурациями программно-аппаратных средств;

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

5.3. Операторы финансовой платформы должны обеспечивать выполнение следующих требований к операционной надежности в отношении выявления, регистрации, реагирования на инциденты операционной надежности и восстановление выполнения технологических процессов и функционирования программно-аппаратных средств после реализации таких инцидентов:

выявление и регистрацию инцидентов операционной надежности, в том числе 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 оператора

финансовой платформы, а также между оператором финансовой платформы 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. Операторы финансовой платформы должны обеспечивать выполнение следующих требований к операционной надежности в отношении взаимодействия с поставщиками услуг:

управление риском реализации информационных угроз при привлечении поставщиков услуг, в том числе защиту программно-аппаратных средств от возможной реализации информационных угроз, включая компьютерные атаки, со стороны поставщиков услуг;

управление риском технологической зависимости функционирования программно-аппаратных средств оператора финансовой платформы от поставщиков услуг;

предотвращение возможной реализации информационных угроз при сопровождении и техническом обслуживании программно-аппаратных средств оператора финансовой платформы поставщиками услуг.

5.5. Операторы финансовой платформы в отношении тестирования операционной надежности технологических процессов должны принимать организационные и технические меры, направленные на разработку сценарного анализа и проведение с использованием сценарного анализа тестирования готовности оператора финансовой платформы противостоять реализации информационных угроз в отношении критичной архитектуры.

5.6. Операторы финансовой платформы в отношении управления риском внутреннего нарушителя должны принимать организационные и технические меры в отношении субъектов доступа, являющихся работниками финансовой организации и работниками поставщиков услуг, привлекаемых в рамках выполнения технологических процессов, направленные на управление

риском реализации информационных угроз, обусловленным возможностью несанкционированного использования предоставленных указанным субъектам доступа полномочий.

5.7. Операторы финансовой платформы должны обеспечивать выполнение следующих требований к операционной надежности в отношении обеспечения осведомленности об актуальных информационных угрозах:

организацию взаимодействия оператора финансовой платформы 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 бесперебойного функционирования программно-аппаратных средств.

6. Оператор финансовой платформы должен обеспечить управление риском возникновения зависимости обеспечения операционной надежности от субъектов доступа, обладающих уникальными знаниями, опытом и компетенцией, а также защиту критичной архитектуры от возможной реализации информационных угроз при организации дистанционной работы работников.

7. Оператор финансовой платформы устанавливает в документах, определяющих правила управления рисками, связанными с деятельностью оператора финансовой платформы, описание процедур, направленных на реализацию требований к операционной надежности, установленных настоящим Указанием, включая:

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

определение организационной структуры оператора финансовой платформы, задействованной в выполнении требований к операционной надежности, в том числе обеспечивающее установление функций подразделений оператора финансовой платформы (в том числе в части

принятия решений с учетом исключения конфликта интересов) и контроль за выполнением требований к операционной надежности в рамках порядка организации и осуществления оператором финансовой платформы внутреннего контроля;

выделение ресурсного обеспечения для выполнения требований к операционной надежности;

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

Оператор финансовой платформы обеспечивает планирование и реализацию требований к операционной надежности начиная с разработки и планирования внедрения технологических процессов.

8. В целях реализации требований к операционной надежности оператор финансовой платформы:

моделирует информационные угрозы в отношении критичной архитектуры;

планирует применение организационных и технических мер, направленных на реализацию требований к операционной надежности, на основе результатов оценки риска реализации информационных угроз в рамках системы управления рисками;

обеспечивает реализацию требований к операционной надежности на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации программно-аппаратных средств;

обеспечивает контроль соблюдения требований к операционной надежности в отношении элементов критичной архитектуры.

Операторы финансовой платформы должны устанавливать во внутренних документах порядок регистрации инцидентов операционной надежности. По каждому инциденту операционной надежности операторы финансовой платформы должны обеспечивать регистрацию:

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.

9. Операторы финансовой платформы 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 информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный оператором финансовой платформы 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.

Операторы финансовой платформы должны предоставлять в Банк России указанные сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия операторов финансовой платформы с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России операторы финансовой платформы 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».

10. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 18 декабря 2020 года № ПСД-30) вступает в силу с 1 октября 2021 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина