Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«___» _____ 202_ г. №_____ -П

г. Москва

Об установлении требований к операционной надежности при совершении финансовых сделок с использованием финансовой платформы

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) (далее – Федеральный закон «О совершении финансовых сделок с использованием финансовой платформы»), настоящее Положение устанавливает требования к операционной надежности при совершении финансовых сделок с использованием финансовой платформы.

1. Требования к операционной надежности при совершении финансовых сделок с использованием финансовой платформы должны применять операторы финансовой платформы в целях обеспечения бесперебойного функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники,

телекоммуникационного оборудования, эксплуатация и использование которых обеспечиваются оператором финансовой платформы для осуществления его деятельности (далее - объекты информационной инфраструктуры), принимаемые оператором финансовой платформы в случаях возникновения нестандартных ситуаций, в том числе при реализации информационных угроз, которые могут препятствовать нормальному осуществлению деятельности оператора финансовой платформы, и направленные на обеспечение непрерывности такой деятельности.

2. Операторы финансовой платформы должны обеспечить пороговый уровень допустимого времени простоя и (или) деградации технологических процессов, обеспечивающих совершение финансовых сделок с использованием финансовой платформы (далее –технологические процессы) не более 2 часов.

3. Операторы финансовой платформы должны определить следующие целевые показатели операционной надежности:

допустимое время простоя и (или) деградации технологических процессов с учетом порогового уровня, установленного в пункте 2 настоящего Положения;

допустимое отношение общего количества финансовых сделок, заключенных во время простоя или деградации технологических процессов в рамках отдельного инцидента, связанного с реализацией информационных угроз, в случае превышения допустимого времени простоя и (или) деградации технологических процессов, к ожидаемому количеству финансовых сделок за тот же период в случае бесперебойного функционирования объектов информационной инфраструктуры, рассчитанное на основе статистических данных за период не менее одного года (далее - доля деградации технологических процессов);

режим работы (функционирования) финансовой платформы (например, 24/7/365).

Операторы финансовой платформы должны обеспечивать контроль за

значениями следующих фактических показателей операционной надежности:

фактическое время простоя и (или) деградации технологических процессов в рамках отдельного инцидента, связанного с реализацией информационных угроз, свыше допустимого времени простоя и (или) деградации технологических процессов;

фактическое количество случаев превышения допустимого времени простоя и (или) деградации технологических процессов;

фактическую долю деградации технологических процессов в рамках отдельного инцидента, связанного с реализацией информационных угроз;

фактический режим работы (функционирования) финансовой платформы.

4. Определение целевых показателей и обеспечение контроля за значениями фактических показателей операционной надежности реализуется оператором финансовой платформы в рамках системы управления рисками.

Оператор финансовой платформы должен проводить регулярный (не реже одного раза в год) анализ необходимости пересмотра показателей операционной надежности.

5. Оператор финансовой платформы должен обеспечить выполнение требований к операционной надежности в рамках следующих процессов (направлений) операционной надежности (далее – процессы операционной надежности):

идентификация состава элементов, указанных в подпункте 5.1 настоящего пункта (далее – критичная архитектура);

управление изменениями критичной архитектуры;

управление конфигурациями и уязвимостями объектов информационной инфраструктуры, входящих в состав критичной архитектуры;

выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление выполнения технологических процессов и функционирования объектов информационной инфраструктуры после их реализации;

взаимодействие с внешними контрагентами, оказывающими услуги в сфере информационных технологий, в рамках которых осуществляется выполнение отдельных технологических процессов оператора финансовой платформы (далее – поставщики услуг);

тестирование операционной надежности технологических процессов;

управление риском несанкционированного доступа работников оператора финансовой платформы или работников поставщиков услуг, обладающих полномочиями доступа к объектам информационной инфраструктуры (далее – внутренний нарушитель);

обеспечение осведомленности об актуальных информационных угрозах.

5.1. Операторы финансовой платформы в рамках идентификации критичной архитектуры должны обеспечивать организацию учета и контроля состава элементов критичной архитектуры.

В состав критичной архитектуры должны включаться следующие элементы:

технологические процессы, реализуемые непосредственно оператором финансовой платформы;

технологические процессы, реализуемые поставщиками услуг;

подразделения оператора финансовой платформы, ответственные за разработку методологии технологических процессов и поддержание их выполнения (далее – подразделения-владельцы);

подразделения оператора финансовой платформы, являющиеся участниками технологических процессов (далее – подразделения-участники);

технологические участки (этапы) технологических процессов;

объекты информационной инфраструктуры оператора финансовой платформы, задействованные при выполнении каждого технологического процесса;

работники оператора финансовой платформы или иные лица, осуществляющие физический и (или) логический доступ, или программные сервисы, осуществляющие логический доступ к объектам информационной

инфраструктуры (далее - субъекты доступа), задействованные при выполнении каждого технологического процесса;

взаимосвязи и взаимозависимости между оператором финансовой платформы, участниками финансовой платформы, регистратором финансовых транзакций, а также поставщиками услуг в рамках выполнения технологических процессов (далее при совместном упоминании – причастные стороны), в том числе взаимосвязей и взаимозависимостей между объектами их информационной инфраструктуры;

объекты информационной инфраструктуры поставщиков услуг, задействованные при выполнении технологических процессов;

потоки защищаемой информации, обрабатываемой в рамках технологических процессов как работниками оператора финансовой платформы, так причастными сторонами при взаимодействии с работниками оператора финансовой платформы.

5.2. Операторы финансовой платформы в рамках управления изменениями критичной архитектуры должны обеспечивать принятие организационных и технических мер, направленных на:

предотвращение возникновения уязвимостей в критичной архитектуре для реализации информационных угроз и нарушения показателей операционной надежности;

планирование и применение изменений в критичной архитектуре, направленных на обеспечение бесперебойного функционирования объектов информационной инфраструктуры.

5.3. Операторы финансовой платформы в рамках управления конфигурациями и уязвимостями объектов информационной инфраструктуры, входящих в состав критичной архитектуры, должны обеспечивать принятие организационных и технических мер, направленных на:

управление конфигурациями объектов информационной инфраструктуры, входящих в критичную архитектуру;

управление уязвимостями и обновлениями (исправлениями) объектов информационной инфраструктуры, входящих в критичную архитектуру

5.4. Операторы финансовой платформы в рамках выявления, регистрации, реагирования на инциденты, связанные с реализацией информационных угроз, и восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после их реализации должны обеспечивать принятие организационных и технических мер, направленных на:

выявление и регистрацию инцидентов, связанных с реализацией информационных угроз, в том числе обнаружение компьютерных атак и фактов компрометации объектов информационной инфраструктуры, входящих в критичную архитектуру;

организацию, координацию и выполнение действий в рамках реагирования на инциденты, связанные с реализацией информационных угроз в отношении критичной архитектуры;

организацию, координацию и выполнение действий в рамках восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации инцидентов, связанных с реализацией информационных угроз в отношении критичной архитектуры;

организацию и проведение анализа причин и последствий реализации инцидентов, связанных с реализацией информационных угроз в отношении критичной архитектуры;

организацию взаимодействия между подразделениями оператора финансовой платформы, а также оператора финансовой платформы с причастными сторонами, Банком России в рамках реагирования на инциденты, связанные с реализацией информационных угроз, и восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после их реализации.

5.5. Операторы финансовой платформы в рамках взаимодействия с

поставщиками услуг должны обеспечивать принятие организационных и технических мер, направленных на:

защиту объектов информационной инфраструктуры, входящих в критичную архитектуру, от возможной реализации информационных угроз, в том числе компьютерных атак, со стороны поставщиков услуг;

управление риском реализации информационных угроз при привлечении поставщиков услуг;

управление риском технологической зависимости функционирования объектов информационной инфраструктуры от поставщиков услуг;

организацию сопровождение и техническое обслуживание объектов информационной инфраструктуры.

5.6. Операторы финансовой платформы в рамках тестирования операционной надежности технологических процессов должны обеспечивать принятие организационных и технических мер, направленных на сценарный анализ и тестирование готовности оператора финансовой платформы противостоять реализации информационных угроз в отношении критичной архитектуры.

5.7. Операторы финансовой платформы в рамках управления риском внутреннего нарушителя должны обеспечивать принятие организационных и технических мер в отношении субъектов доступа, входящих в состав критичной архитектуры, являющихся работниками финансовой организации и работниками поставщиков услуг, привлекаемых в рамках выполнения и технологических процессов. Принимаемые организационные и технические меры должны обеспечить управление риском реализации информационных угроз, обусловленного возможностью неправомерного использования предоставленных субъектам доступа полномочий.

5.8. Операторы финансовой платформы в рамках обеспечения осведомленности об актуальных информационных угрозах должны обеспечивать принятие организационных и технических мер, направленных на:

организацию и выполнение деятельности по получению от причастных сторон и направлению причастным сторонам информации об актуальных

сценариях реализации информационных угроз, включая результаты анализа причин инцидентов, связанных с реализацией информационных угроз, и последствий от их реализации (далее - информация об актуальных сценариях реализации информационных угроз);

организацию и выполнение деятельности по получению от Банка России и направлению в Банк России информации об актуальных сценариях реализации информационных угроз с использованием технической инфраструктуры (автоматизированной системы) Банка России;

использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения бесперебойного функционирования объектов информационной инфраструктуры, входящих в состав критичной архитектуры.

6. Оператор финансовой платформы в дополнение к выполнению указанных в пункте 5 требований к операционной надежности в рамках процессов операционной надежности 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 удаленной работы сотрудников.

7. Оператор финансовой платформы в рамках реализуемой им системы управления рисками определяет в документах, регламентирующих процедуры управления рисками, описание состава деятельности по организации применения процессов операционной надежности, включая:

определение и описание состава процессов операционной надежности, а также целевого уровня зрелости (меры оценки полноты, адекватности и эффективности выполнения процессов операционной надежности) таких процессов;

определение организационных и технических мер, применяемых в рамках процессов операционной надежности, а также области применения таких

процессов в отношении критичной архитектуры;

определение организационной структуры оператора финансовой платформы, задействованной в реализации процессов операционной надежности, в том числе обеспечивающей контроль за реализацией процессов операционной надежности со стороны исполнительного органа оператора финансовой платформы;

выделение ресурсного обеспечения для реализации процессов операционной надежности;

порядок утверждения и условия пересмотра состава деятельности по организации применения процессов операционной надежности.

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

Оператор финансовой платформы обеспечивает установление функций подразделений-владельцев и подразделений-участников, ролей и обязанностей среди лиц (в том числе в части принятия решений с учетом исключения конфликта интересов), в компетенцию которых входит реализация процессов операционной надежности, с учетом утвержденного состава деятельности по организации применения.

Для цели реализации процессов операционной надежности оператор финансовой платформы обеспечивает функционирование постоянно действующего комитета (группы) для реализации механизма взаимодействия и координации подразделений-владельцев и подразделений-участников, а также причастных сторон.

8. Для цели реализации требований к процессам операционной надежности оператор финансовой платформы:

моделирует информационные угрозы в отношении критичной архитектуры;

планирует применение организационных и технических мер, направленных на реализацию требований к процессам операционной

надежности, в том числе на основе результатов оценки риска реализации информационных угроз в рамках системы управления рисками;

обеспечивает реализацию, контроль и совершенствование применения организационных и технических мер, направленных на реализацию требований к процессам операционной надежности;

обеспечивает применение процессов операционной надежности на этапах жизненного цикла объектов информационной инфраструктуры;

обеспечивает соответствие полноты и качества процессов операционной надежности целевому уровню зрелости, установленному в рамках состава деятельности по организации применения процессов операционной надежности;

определяет и обеспечивает контроль требований к обеспечению операционной надежности в рамках взаимодействия с причастными сторонами.

9. Операторы финансовой платформы к инцидентам, связанным с реализацией информационных угроз, приведшим к нарушению показателей операционной надежности (далее - инциденты операционной надежности), должны относить события, которые привели или могут привести к нарушению бесперебойного функционирования объектов информационной инфраструктуры, в том числе включенные в перечень типов инцидентов, размещаемый Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее соответственно – сеть «Интернет», перечень типов инцидентов).

Операторы финансовой платформы устанавливают во внутренних документах порядок регистрации инцидентов операционной надежности. Сведения об инцидентах операционной надежности направляются в службу управления рисками в целях включения их в базу событий операционного риска в порядке, установленном внутренними документами оператора финансовой платформы.

Операторы финансовой платформы должны обеспечивать регистрацию инцидентов операционной надежности.

По каждому инциденту операционной надежности операторы финансовой платформы должны обеспечивать регистрацию:

даты, времени, длительности нарушения бесперебойного функционирования объектов информационной инфраструктуры;

данных, позволяющих выявить причину нарушения бесперебойного функционирования объектов информационной инфраструктуры;

результата реагирования на инцидент операционной надежности.

10. Операторы финансовой платформы должны информировать Банк России:

о выявленных самостоятельно или Банком России инцидентах операционной надежности, включенных в перечень типов инцидентов, 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 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».

11. Настоящее Положение в соответствии с решением Совета

директоров Банка России (протокол заседания Совета директоров Банка России от _____ 2020 года № __) вступает в силу по истечении 360 дней после дня его официального опубликования.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина