Утверждено
Приказом генерального директора №13/2023
от «13» апреля 2023 года

Порядок контроля операционной надежности и мониторинга операционных рисков в целях обеспечения непрерывности оказания финансовых услуг ООО «СИМПЛ ЭСТЭЙТ»

г. Москва, 2023 год

Оглавление

1. Общие положения

1.1. Порядок контроля операционной надежности и мониторинга операционных рисков в целях обеспечения непрерывности оказания финансовых услуг (далее – Порядок) является внутренним документом ООО «СИМПЛ ЭСТЭЙТ» (далее - Организация), разработанным в целях исполнения требований Положения Банка России от 15 ноября 2021 г. № 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 № 779-П).

1.2. Настоящий Порядок разработан в соответствии с:

– Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ);

– Положением Банка России от 15 ноября 2021 г. № 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)»;

– Указом Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Методическими рекомендациями Банка России по обеспечению непрерывности деятельности некредитных финансовых организаций от 18 августа 2016 г. № 28-МР;

– Внутренними документами Организации, регламентирующими систему управления рисками и устанавливающими требования к защите информации;

– ГОСТ Р 57580.3-2022 Безопасность финансовых (банковских) операций. Управление рисков реализации информационных угроз и обеспечение операционной надежности. Общие положения.

– ГОСТ Р 57580.4-2022 Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер.

1.3. Процедуры управления операционным риском, регулируемые настоящим Порядком, включаются в общую Систему управления рисками (СУР), действующую в Организации, включая ведение Реестра рисков.

1.4. Организация использует настоящий Порядок для контроля операционных рисков в соответствии с требованиями законодательства в сфере управления рисками, в том числе рисками информационных угроз.

1.5. Результаты мониторинга и обработки операционных рисков отражаются в регулярной отчетности, предусмотренной СУР и формируемой в установленном порядке согласно внутреннему документу Организации [Положение по управлению рисками], регламентирующего функционирование системы управления рисками.

1.6. Определения, используемые в настоящем Порядке:

Операционная надежность (в условиях возможной реализации информационных услуг); киберустойчивость – способность Организации обеспечивать непрерывность функционирования бизнес- и технологических процессов с учетом целевых показателей операционной надежности в условиях возможной реализации информационных угроз;

Техническая мера обеспечения операционной надежности – мера, реализуемая с помощью применения аппаратных, программных, аппаратно-программных средств и (или) систем;

Организационная мера обеспечения операционной надежности – мера, не являющаяся технической мерой обеспечения операционной надежности, предусматривающая установления регламента работы с элементами критичной архитектуры и порядка фиксации результатов выполненной работы, в том числе установление в отдельных случаях временных, территориальных, пространственных, правовых, методических и иных ограничений на условиях использования, и режимы работы объекта информатизации и (или) иных связанных с ним объектов;

Система управления рисками (СУР) - совокупность процессов, методик, информационных систем, направленных на достижение целей и задач управления рисками;

Риск реализации информационных угроз – возможность реализации информационных угроз (в совокупности с последствиями от их реализации), которые обусловлены недостатками процессов обеспечения операционной надежности и защиты информации, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности Организации;

Поставщик услуг (информационных сервисов и услуг) – обслуживающая организация, специализирующаяся на предоставлении информационных сервисов и услуг, в том числе в рамках которых финансовые организации передают выполнение своих бизнес- и технологических процессов на аутсорсинг;

Внутренний нарушитель (безопасность информации) – лицо, в том числе сотрудник Организации, сотрудник поставщиков услуг, реализующие информационные угрозы с использованием легально предоставленных им прав доступа, в том числе с использованием уязвимостей;

Внешний нарушитель (безопасности информации) – лицо, реализующее информационный угрозы без использования легально предоставленных прав доступа, с использованием уязвимостей;

Уязвимость – недостаток применения технологических мер защиты информации, применяемых объектов информатизации прикладного уровня, недостаток планирования, реализации, контроля и совершенствования процессов управления риском реализации информационных угроз, обеспечения операционной надежности и (или) защиты информации, эксплуатация которого позволяет нарушителю безопасности информации реализовать информационные угрозы в отношении критических активов;

Объект информатизации (прикладного и инфраструктурного уровней Организации); объект информационной инфраструктуры – совокупность объектов и ресурсов доступа, средств и систем обработки информации, используемых для обеспечения информатизации бизнес и технологических процессов Организации, используемых для предоставления финансовых и (или) информационных услуг;

Бизнес-процесс и (или) технологический процесс Организации; бизнес и технологический процесс – набор взаимосвязанных операций, в том числе технических, в отношении активов Организации или информации и (или) объектов информатизации, используемых при осуществлении Организацией видов деятельности, связанных с предоставлением финансовых и (или) информационных услуг;

Ключевой индикатор риска реализации информационных угроз (КИР) – количественный показатель, используемый для оперативного измерения и контроля уровня риска реализации информационных угроз в определенный момент времени;

Деградация технологических процессов - нарушения технологических процессов, приводящие к неоказанию или ненадлежащему оказанию финансовых услуг клиентам;

Инцидент (связанный с реализацией информационных угроз) – одно или серия связанных нежелательных событий, связанных с возможной реализацией информационных угроз, которые указывают на свершившуюся, предпринимаемую или вероятную реализацию информационных угроз;

Система организации и управления операционной надежностью – совокупность мер, применением которых достигается полнота и качество обеспечения операционной надежности, предназначенных для планирования, реализации, контроля и совершенствования процессов системы обеспечения операционной надежности;

Информационная угроза; угроза безопасности информации – совокупность условий и факторов, побуждающих клиента Организации к осуществлению финансовых (банковских) операций, в том числе операций по переводу денежных средств путем обмана или злоупотреблением доверия, и (или) создающих возможность нарушения безопасности информации, вызывающую или способную вызвать негативные последствия (включая нарушение операционной надежности) для Организации, причастных сторон, в том числе клиентов Организации;

Источник риска реализации информационных угроз – объект или деятельность, которые самостоятельно или в комбинации с другими обладают возможностью вызывать или повышать уровень риска реализации информационных угроз;

Компьютерная атака – вид информационной угрозы, заключающийся в преднамеренных действиях со стороны сотрудников Организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, в том числе штатных, направленных на критические активы;

Политика информационной безопасности – общее намерение и направление, официально устанавливаемое органом управления Организации.

2. Управление риском информационных угроз

2.1. Организация на постоянной основе осуществляет управление риском информационных угроз с целью поддержания операционной надежности (киберустойчивости).

2.2. Организация использует организационные и технические меры обеспечения операционной надежности для защиты собственных объектов информационной инфраструктуры от возможной реализации информационных угроз со стороны поставщиков услуг, внешних и внутренних нарушителей, иных источников риска реализации информационных угроз.

2.3. Система управления рисками (СУР) Организации включает в себя контроль ключевых индикаторов риска (КИР) операционного риска, включающего в себя риск реализации информационных угроз в отношении объектов информационной инфраструктуры и технологических процессов Организации.

2.4. Организация определяет и контролирует риск технологической зависимости функционирования своих объектов информационной инфраструктуры от поставщиков услуг.

2.5. Степень влияния риска реализации информационных угроз на объекты информационной инфраструктуры и технологические процессы определяется в соответствии с п. 4.3 настоящего Порядка.

2.6. Организация принимает организационные и технические меры в отношении своих сотрудников и сотрудников поставщиков услуг, привлекаемых в рамках выполнения технологических процессов, направленные на управление риском реализации информационных угроз, что обусловлено возможностью несанкционированного использования доступа к защищаемой информации. Информирование указанных лиц осуществляется посредством размещения в неограниченном доступе внутреннего документа Организации [Политики информационной безопасности]. Основные мероприятия предусмотрены во внутреннем документе Организации, который разработан в целях организации режима защиты информации, содержащей сведения конфиденциального характера, в том числе получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах [Положение об обеспечении защиты сведений конфиденциального характера]. При этом Организация учитывает риск возникновения зависимости обеспечения операционной надежности от субъектов доступа - сотрудников, обладающих знаниями, опытом и компетенцией.

2.7. Руководитель Организации контролирует обеспечение защиты критичной архитектуры и технологических процессов от возможной реализации информационных угроз в периоды выполнения сотрудниками Организации трудовой функции дистанционно.

2.8. Организация проводит взаимодействие с прочими участниками технологических процессов при обмене информацией об актуальных сценариях реализации информационных угроз для использования данной информации с целью обеспечения непрерывности оказания финансовых услуг.

2.9. В случае отнесения Организации к системно значимым инфраструктурным организациям финансового рынка на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») и которые являются субъектами критической информационной инфраструктуры в соответствии с пунктом 8 статьи 2 Федерального закона № 187-ФЗ, Организация должна выполнять требования, направленные на противодействие целевым компьютерным атакам, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в зависимости от уровня опасности.

2.10. Для оценки уровня риска информационных угроз сотрудник, ответственный за управление операционным риском, проводит оценку и расчет индикаторов операционной надежности в соответствии с п. 3.4 настоящего Порядка.

3. Индикаторы операционной надежности

3.1. Организация осуществляет контроль пороговых уровней показателей операционной надежности (далее - базовые показатели) с целью выявления и минимизации инцидентов, связанных с реализацией информационных угроз. К базовым показателям относятся:

П1 - пороговый уровень допустимого времени простоя технологических процессов, обеспечивающих осуществление деятельности в сфере финансовых рынков (далее - технологические процессы), в часах;

П2 - пороговый уровень деградации технологических процессов, в часах.

3.2. Организация устанавливает и контролирует следующие целевые показатели операционной надежности в отношении каждого технологического процесса, указанных в Приложении №2 (далее - целевые показатели):

Ф1 - отношение общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг (далее - события операционного риска, связанные с нарушением операционной надежности), к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг (далее - доля деградации технологических процессов), в процентах;

Ф2 - 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), в часах;

Ф3 - 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, в часах;

Ф4 - показатель соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса).

3.3. С целью контроля указанных базовых и целевых показателей Организация на ежегодной основе устанавливает квартальные лимиты к ним в соответствии с формой, указанной в Приложении №1 к настоящему Порядку.

3.4. Сотрудник, ответственный за управление операционным риском, на ежеквартальной основе формирует отчетность, включающую в себя контроль лимитов показателей операционной надежности П1, П2, Ф1, Ф2, Ф3, Ф4 для каждого технологического процесса.

3.5. В случае превышения допустимой доли деградации технологических процессов Ф1, сотрудник, ответственный за работу с операционным риском обеспечивает фиксацию:

– фактической доли деградации технологического процесса Ф1, исчисляемой по каждому событию операционного риска, связанному с нарушением операционной надежности;

– фактического времени простоя и (или) деградации технологического процесса Ф2, исчисляемого по каждому событию операционного риска, связанному с нарушением операционной надежности (с момента нарушения технологического процесса по причине

реализации события операционного риска, связанного с нарушением операционной надежности, до момента восстановления выполнения технологического процесса);

– суммарного времени простоя и (или) деградации технологического процесса ФЗ за последние двенадцать календарных месяцев, предшествующих событию операционного риска, связанному с нарушением операционной надежности.

3.6. 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.

3.7. Инциденты риска информационных угроз в рамках контроля операционного риска фиксируются в установленном порядке согласно внутреннему документу [Положение по управлению рисками], регламентирующему функционирование системы управления рисками.

4. Контроль критичной архитектуры

4.1. В целях реализации системы организации и управления операционной надежностью Организация организует учет и контроль следующей критичной архитектуры:

– технологических процессов, реализуемых Организацией, а так же подразделений (сотрудников), ответственных за разработку технологических процессов, поддержание их выполнения, их реализацию;

– технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг;

– сотрудников Организации или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной инфраструктуры Организации (далее - субъекты доступа), задействованных при выполнении каждого технологического процесса;

– каналов передачи защищаемой информации, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса. Соответствующая информация указана в пункте 1.1 Положения Банка России от 20 апреля 2021 года № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» и определена во внутреннем документе Организации, который разработан в целях организации режима защиты информации, содержащей сведения конфиденциального характера, в том числе получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах [Положение об обеспечении защиты сведений конфиденциального характера];

– объектов информационной инфраструктуры Организации, задействованных при выполнении каждого технологического процесса.

4.2. Организация ведет реестр технологических процессов, реализуемых Организацией и поставщиками услуг, а так же объектов информационной инфраструктуры и каналов передачи защищаемой информации согласно форме, определенной в Приложении №2 к настоящему Порядку, с указанием сотрудников, ответственных за реализацию технологических процессов и поддержание их выполнения.

Реестр формируется и актуализируется при необходимости сотрудником, ответственным за управление операционным риском.

4.3. Для каждого объекта критичной архитектуры определяется степень влияния на иные объекты критичной архитектуры согласно форме, указанной в Приложении №3 к настоящему Порядку, что позволяет определить степень влияния указанных элементов критической инфраструктуры друг на друга.

4.4. Для каждого технологического процесса рассчитываются и контролируются целевые индикаторы операционной надежности в соответствии с главой 3 настоящего Порядка, а также фиксируются инциденты риска информационных угроз.

4.5. Организация на ежегодной основе проводит анализ своей критичной архитектуры и исполняет требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ в случае такой необходимости.

4.6. Ответственные сотрудники Организации осуществляют планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение непрерывного оказания финансовых услуг.

4.7. Организация обеспечивает управление конфигурациями объектов информационной инфраструктуры, управление уязвимостями и обновлениями (исправлениями) объектов информационной инфраструктуры.

5. Реализация требований к операционной надежности и обработка операционных рисков критичной архитектуры

5.1. Для целей исполнения настоящего Порядка, а так же в рамках функционирования системы управления рисками (СУР) Организация проводит выявление, регистрацию и анализ событий операционного риска, связанных с нарушением операционной надежности.

5.2. Организационная структура, задействованная в исполнении требований к операционной надежности, определяется в рамках системы управления рисками (СУР) соответствующими регламентирующими и распорядительными документами Организации с обеспечением исключения конфликта интересов и осуществлением Организацией внутреннего контроля (в случае его наличия).

5.3. В рамках осуществления процедур реагирования на риск, включенных в Реестр рисков СУР, Организацией разрабатываются и проводятся мероприятия по снижению уровня риска, а также мероприятия по восстановлению нормального течения и исполнения технологических процессов.

5.4. Сотрудники, отвечающие за соответствующие технологические процессы, организуют взаимодействие между подразделениями (сотрудниками) Организации, ответственными за разработку, поддержание их выполнения и реализацию технологических процессов между собой, иными участниками технологического процесса и Банком России.

5.5. Организация обеспечивает анализ причин и последствий реализации событий операционного риска, связанных с нарушением операционной надежности в соответствии с формой, указанной в Приложении №4 к настоящему Порядку, с целью оптимизации остаточного уровня риска критичной архитектуры. Сотрудник, ответственный за управление операционным риском, в случае необходимости готовит предложения о

выделении необходимого ресурсного обеспечения для выполнения требований к операционной надежности.

5.6. Организация проводит накопление и анализ информации о рисках критичной архитектуры, свершившихся инцидентах риска информационных угроз с целью планирования и внедрения изменений в критичной архитектуре, направленных на обеспечение непрерывного оказания финансовых услуг.

5.7. Сотрудник, ответственный за управление операционным риском, принимает участие в разработке и планировании внедрения технологических процессов, проводит необходимое определение и описание состава процедур, направленных на выполнение требований к операционной надежности в Организации.

5.8. Утверждение и пересмотр процедур, направленных на выполнение требований к операционной надежности, проводится в рамках пересмотра ежегодного Реестра рисков, что предусмотрено [Положением по управлению рисками] и настоящим Порядком.

6. Отчетность, формируемая в рамках контроля операционной надежности

6.1. Для целей мониторинга показателей операционной надежности сотрудник, ответственный за управление операционным риском, на ежеквартальной основе формирует отчет по расчету базовых и целевых индикаторов согласно форме, указанной в Приложении №5 к настоящему Порядку, в соответствии с реестром технологических процессов, зафиксированных в отчете по форме, указанной в Приложении №2 к настоящему Порядку.

6.2. Сотрудник, ответственный за управление операционным риском, контролирует значения лимитов по индикаторам операционной надежности, установленных по форме, указанной в Приложении №1 к настоящему Порядку, и выявляет события операционного риска в случае превышения лимитов.

6.3. Учет и контроль критичной архитектуры ведется согласно форме, указанной в Приложении №3 к настоящему Порядку.

6.4. По каждому выявленному событию нарушения операционной надежности сотрудник, ответственный за управление операционным риском, не позднее следующего рабочего дня заполняет отчет в соответствии с формой, указанной в Приложении №4 к настоящему Порядку, где прописывается перечень проведенных мероприятий по снижению уровня риска и оценка величины остаточного риска.

6.5. Организация формирует отчетность по зафиксированным событиям операционного риска в соответствии с внутренним документом [Положение по управлению рисками], регламентирующим функционирование системы управления рисками.

6.6. В случае отсутствия у Организации внутреннего документа [Положение по управлению рисками] Реестр рисков (план обработки риск-событий) формируется согласно форме, указанной в Приложении №6 к настоящему Порядку.

6.6.1. Реестр рисков является формой записи информации об идентифицированном риске, сроках и способах его обработки, предупреждающих действиях. В Реестр рисков включают все идентифицированные опасные события, выявленные в Организации и ее подразделениях, результат оценки их риска, а также оценку возможных последствий опасного события для деятельности Организации.

6.6.2. Реестр рисков является планом действий, так как в Реестре рисков кроме идентификации опасностей и оценки риска определены необходимые мероприятия по снижению риска, сроки их внедрения и ответственные сотрудники за их выполнение.
6.6.3. Ответственность за подготовку и утверждение Реестра рисков по мере необходимости, но не реже 1 (одного) раза в год возлагается на сотрудника, выполняющего функции риск-менеджера в Организации.

7. Заключительные положения

7.1. Настоящий Порядок утверждается руководителем Организации и обязателен для соблюдения всеми сотрудниками Организации.
7.2. Настоящий Порядок пересматривается сотрудником, выполняющим функции риск-менеджера в Организации, по мере необходимости, но не реже одного раза в год в целях актуализации содержащихся в них сведений и (или) повышения эффективности функционирования СУР Организации.

Приложение №1

Лимиты индикаторов риска базовых показателей на ____ год

№	Ключевой индикатор	Лимит на квартал	Значение	Примечание
1	П1			
2	П2			

Лимиты индикаторов риска целевых показателей на ____ год для технологического процесса _____

№	Ключевой индикатор	Лимит на квартал	Значение	Примечание
1	Ф1			
2	Ф2			
3	Ф3			
4	Ф4			

Приложение №2

Реестр технологических процессов, реализуемых Организацией и поставщиками услуг, а так же объектов информационной инфраструктуры и каналов передачи защищаемой информации (список объектов критичной архитектуры)

№	Наименование технологического процесса	Ответственный сотрудник Организации (субъект доступа)	Наличие канала защищаемой информации	Наличие внешнего поставщика	Задействованные объекты информационной инфраструктуры

Приложение №3

Карта взаимного влияния объектов критичной архитектуры

№	Наименование Объекта А критичной архитектуры	Влияние на соответствующий Объект В критичной архитектуры						
		1	2	3	4	5	6	
1								
2								
3								
4								
5								
6								

X	Объект А влияет на Объект В	Неработоспособность/деградация А ведет к неработоспособности/деградации В
0	Объект А не влияет на Объект В	Влияние отсутствует
?	Влияние Объекта А на Объект В невозможно определить и документировать	

Приложение №4

Отчет о факте нарушения операционной надежности

№		
1	Объект критичной архитектуры	
2	Краткое описание инцидента	
3	Ответственный сотрудник	
4	Оценка влияния на базовые показатели операционной надежности	
5	Оценка влияния на целевые показатели операционной надежности	
6	Выводы о нарушении лимитов	
7	Выводы о наличии риск-инцидента	
8	Отметка о выполнении мероприятий	
9	Выводы о величине остаточного риска	

Ответственный сотрудник:
Дата:

Приложение №5

Расчет базовых индикаторов операционной надежности за ___ квартал

№	Ключевой индикатор	Лимит на квартал	Значение за квартал	Отклонение
1	П1			
2	П2			

Расчет целевых индикаторов операционной надежности за ____ квартал для технологического процесса _____

№	Ключевой индикатор	Лимит на квартал	Значение	Отклонение
1	Ф1			
2	Ф2			
3	Ф3			
4	Ф4			

Приложение №6

Реестр рисков на ____ год

Порядковый номер	Описание риска	Источники (факторы) риска	Триггер (условие идентификации риска)	Возможные последствия риска. Влияние риска на деятельность Организации	Оценка вероятности реализации риска	Влияние риска на другие риски	Мероприятия и/или процедуры по управлению риском	Лицо и/или подразделение ответственное за проведение и учет операций, подверженных рискам	Лицо и/или подразделение, ответственное за мероприятия по управлению данным риском (владелец риска)	Перечень источников информации, используемых для идентификации и оценки риска	Примечание
1											
2											