УТВЕРЖДЕНО
Решением единственного акционера
Акционерного общества
«Универсальные Финансовые Технологии»
№ 3 от «05» сентября 2023 г.

ПРАВИЛА УПРАВЛЕНИЯ РИСКАМИ
Акционерного общества
«Универсальные Финансовые Технологии»

Вступает в силу	
Редакция №	1

2023 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан и утвержден в Акционерном обществе «Универсальные Финансовые Технологии» (АО «УФТ», далее – Общество, Оператор ФП) в соответствии с Федеральным законом от 20.07.2020 года №211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы».

1.2. Настоящие Правила управления рисками Акционерного общества «Универсальные Финансовые Технологии» (далее - Правила) определяют цели, задачи, принципы и процедуры управления рисками, а также организацию управления рисками в Акционерном обществе «Универсальные Финансовые Технологии».

1.3. Правила разработаны в соответствии с законодательством Российской Федерации, а также внутренними нормативными документами Общества и распространяются на все его структурные подразделения.

1.4. Предусмотренные Правилами подходы к управлению рисками Общества соответствуют принципам, изложенным в международных стандартах по управлению рисками ISO 31000:2018.

1.5. Правила содержат описание основных рисков, а также описывают основные процедуры по управлению данным рисками.

1.6. Общество обеспечивает хранение документов и информации, связанных с управлением рисками, не менее чем за 5 (пять) лет со дня их создания.

1.7. Общество не совмещает свою деятельность с деятельностью кредитной организации, бюро кредитных историй или иной некредитной финансовой организацией.

1.8. Общество осуществляет постоянное развитие и совершенствование системы управления рисками для снижения уязвимости процессов Общества и времени их восстановления, повышения уровня резервирования технологий на основе принципа разнесения и дублирования ресурсов.

2. ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

Банк России - Центральный банк Российской Федерации, включая его территориальные подразделения.

БС/БСР – База событий по рискам. Представляет собой общий реестр с событиями рисков, в разрезе видов рисков, присущих Обществу.

Единоличный исполнительный орган – Генеральный директор Акционерного общества «Универсальные Финансовые Технологии» и (или) лицо его замещающее, на основании организационно-распорядительного документа.

Значимые риски – риски, негативные последствия реализации которых оказывают существенное влияние на финансовый результат Общества и (или) репутацию Общества либо на возможность соблюдения требований регулирующих органов Российской Федерации. Признание риска значимым влечет за собой обязательность принятия мер по управлению данным риском.

Идентификация риска – процесс выявления присущих и потенциальных видов/подвидов риска и оценка степени их материальности (вероятности возникновения и существенности влияния для Общества).

Операционный риск (далее - ОР) - риск возникновения последствий, влекущих за собой приостановление или прекращение оказания услуг в полном или неполном объеме, а также риском

возникновения расходов (убытков) Оператора ФП в результате сбоев и (или) ошибок программно-технических средств, и (или) во внутренних бизнес-процессах, ошибок работников и (или) в результате внешних событий, оказывающих негативное воздействие на Оператора ФП.

Оценка риска – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и (или) совокупных рисков, принимаемых на себя Обществом.

Риск – присущая деятельности Общества возможность (вероятность) возникновения потерь и (или) возникновения иных негативных последствий вследствие наступления неблагоприятных событий, связанных как с внутренними факторами Общества, так и внешними факторами (изменение экономических условий, применяемые технологии, действия регулирующих органов и т. д.).

Регуляторный (комплаенс) риск - риск возникновения у Оператора ФП расходов (убытков) и (или) иных неблагоприятных последствий в результате несоответствия деятельности требованиям федеральных законов и принятых в соответствии с ними нормативных актов, правилам Оператора ФП, учредительным и внутренним документам Оператора ФП, а также в результате применения санкций и (или) мер воздействия со стороны Банка России, других регулирующих или контролирующих органов.

Риск потери деловой репутации - риск возникновения негативных последствий у Оператора ФП в результате негативного восприятия Оператора ФП со стороны Потребителей, контрагентов, Финансовых организаций, Банка России и иных лиц, которые могут негативно повлиять на способность Оператора ФП поддерживать существующие и (или) устанавливать новые деловые отношения и поддерживать на постоянной основе доступ к источникам финансирования.

Самооценка - направленный на снижение уровня рисков процесс проведения самостоятельного выявления и оценки структурным подразделением Общества всех присущих подразделению рисков, определения уровня и значимости рисков в процессах своего подразделения на основе формализованных анкет.

Санкционный риск – вероятность того, что в отношении контрагента, его учредителя, бенефициара или контролирующего лица будут введены американские или европейские санкции, что не позволит продолжить исполнение договора без ограничений.

Стратегический риск - риск возникновения расходов (убытков) в результате принятия неправильных решений в процессе планирования и управления, в том числе при разработке, утверждении и исполнении документов, определяющих направления развития, и(или) при ненадлежащем исполнении принятых решений в процессе управления.

СМИ – средства массовой информации.

СУР – Служба управления рисками Акционерного общества «Универсальные Финансовые Технологии», являющаяся самостоятельным структурным подразделением, ответственным за управление рисками Общества.

Общество - Акционерное общество «Универсальные Финансовые Технологии» (АО «УФТ»).

Оператор финансовой платформы (Оператор ФП) - Акционерное общество «Универсальные Финансовые Технологии» (АО «УФТ»). Юридическое лицо, созданное в организационно-правовой форме акционерного общества в соответствии с законодательством Российской Федерации, оказывающее услуги, связанные с обеспечением возможности совершения Финансовых сделок между Финансовыми организациями и Потребителями с использованием финансовой платформы, включенное в реестр операторов финансовых платформ Банка России.

Оперативный штаб – Созываемая в экстренном режиме, либо по решению Единоличного исполнительного органа группа оперативного реагирования, состоящая из руководителей

структурных подразделений Общества, имеющих функции принятия решений в рамках своей компетенции, согласно должностным инструкциям и внутренним документам Общества.

ПОД/ФТ/РОМУ - противодействие легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и распространения оружия массового уничтожения.

Потребитель (Потребитель финансовых услуг) - Физическое лицо, являющееся потребителем финансовых услуг и соответствующее требованиям, установленным Правилами финансовой платформы, присоединившееся к Договору об оказании услуг Оператора финансовой платформы в порядке, установленном Правилами финансовой платформы, в целях совершения Финансовых сделок. Потребителем считается Авторизовавшийся пользователь.

Управление рисками – выявление, оценка и агрегирование значимых видов рисков, иных видов рисков, которые в сочетании со значимыми могут привести к потерям, существенно влияющим на оценку достаточности капитала.

Финансовые организации (ФО) - кредитные организации, присоединившиеся к договору об оказании услуг Оператора финансовой платформы, условия которого установлены Правилами финансовой платформы, в целях совершения Финансовых сделок с Потребителями финансовых услуг.

Финансовая платформа (Платформа) - информационная система, использующая программно-аппаратные средства, предназначенные для обеспечения взаимодействия Потребителей и Финансовых организаций посредством информационно – телекоммуникационной сети «Интернет» в целях обеспечения возможности совершения Финансовых сделок, доступ к которой предоставляется Оператором финансовой платформы.

Финансовый риск - риск возникновения убытков вследствие неисполнения, несвоевременного либо неполного исполнения контрагентом своих обязательств в соответствии с условиями договоров.

Финансовая сделка - сделка, совершаемая между Потребителями и Финансовыми организациями с использованием Финансовой платформы. Перечень финансовых сделок, заключение (совершение) которых возможно с использованием Финансовой платформы, устанавливается Правилами финансовой платформы.

3. ЦЕЛИ И ЗАДАЧИ УПРАВЛЕНИЯ РИСКАМИ

3.1. Основными целями системы управления рисками являются:

- Управление рисками, в том числе с целью их минимизации и устранения;
- Обеспечение нормального функционирования Общества в рамках возможных нестандартных и чрезвычайных ситуаций;
- Планирование деятельности Общества, в том числе исходя из результатов всесторонней оценки основных рисков;
- Выполнение требований государственных органов Российской Федерации, регулирующих деятельность Общества.

3.2. Основными задачами системы управления рисками являются:

- Выявление, оценка, агрегирование значимых рисков и иных видов рисков, которые в сочетании со значимыми рисками, могут привести к потерям, существенно влияющим на способность Общества поддерживать свою деятельность;

- Своевременная идентификация источников рисков (как в существующих, так и во внедряемых новых продуктах, операциях, автоматизированных системах и технологиях);
- Количественная и качественная оценка рисков, анализ и контроль их влияния на финансовую устойчивость Общества и результаты его деятельности;
- Мониторинг рисков, присущих деятельности Общества;
- Мониторинг влияния рисков на финансовую устойчивость, достижение стратегических и операционных целей, непрерывность деятельности и операционную надежность, а также деловую репутацию Общества;
- Разработка, реализация и оценка эффективности методов ограничения или снижения уровня рисков;
- Предотвращение реализации рисков и снижение их последствий до приемлемого для Общества уровня;
- Своевременная постановка вопросов и выявление проблем, требующих рассмотрения и решения на соответствующем уровне;
- Информирование заинтересованных сторон по вопросам управления рисками и их текущего уровня;
- Развитие и распространение корпоративной культуры управления рисками;
- Построение эффективной системы управления рисками.

4. ОСНОВНЫЕ ПРИНЦИПЫ ЭФФЕКТИВНОГО ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

Основные принципы эффективного функционирования системы управления рисками:

- **Непрерывность.** Процесс управления рисками осуществляется на постоянной основе и представляет собой набор процедур по оценке текущих рисков, выявлению потенциальных рисков и анализ процесса управления рисками.
- **Независимость функции управления рисками.** СУР не участвует в совершении финансовых сделок Оператора финансовой платформы, а также в совершении гражданско-правовых сделок и заключении соглашений. Профессиональная компетентность заключается в том, что СУР должна владеть достаточными знаниями о деятельности Общества для управления и контроля за присущими ему рисками. Система управления рисками строится с учётом предотвращения конфликта интересов в Обществе и принципов независимости любого решения в части принятия принятии рисков, их оценки и осуществления контроля над ними.
- **Информированность.** Управление рисками сопровождается наличием объективной, достоверной и актуальной информации для минимизации риска принятия несвоевременного и неправильного решения. Принятие решения о проведении любой операции производится только после всестороннего анализа рисков, возникающих в результате такой операции.
- **Регламентирование процессов.** Все операции проводятся с соблюдением внутренних нормативных и (или) организационно-распорядительных документов. Проведение новых операций, подверженных существенным рискам, при отсутствии внутренних нормативных, организационно-распорядительных документов не допускается.

- **Вовлеченность и контроль уровня рисков.** Вовлечение заинтересованных сторон в процессы управления рисками позволяет учесть их знания и экспертное мнение. Органы управления Общества своевременно на регулярной основе получают информацию о принятом уровне рисков, и также вовлечены в процесс управления и создания контрольной среды.
- **Открытость.** Принцип открытости подразумевает прозрачность и своевременное предоставление всей необходимой информации об организации системы управления рискам всем заинтересованным сторонам.
- **Экономическая целесообразность.** При внедрении различных элементов системы управления рисками следует исходить из оценки затрат на реализацию механизмов анализа, контроля и управления рисками с ожидаемыми результатами от этой реализации. Стоимость мер минимизации риска должна быть сопоставима с величиной возможных потерь Общества от этого риска.
- **Совершенствование системы управления рисками и постоянное развитие.** Система управления рисками Общества соответствует уровню развития операций Общества, а также внешним условиям, нововведениям в мировой практике управления рисками и специфики деятельности Общества. Процесс управления рисками постоянно совершенствуется благодаря обучению и накоплению опыта.
- **Интегрированность.** Управление рисками является неотъемлемой частью повседневной деятельности Общества. Система и процесс управления рисками формируется с учетом внешней и внутренней структуры Общества, связанной с его основными задачами.

5. ОРГАНИЗАЦИЯ И СТРУКТУРА СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

5.1. Все структурные подразделения и должностные лица Общества могут быть вовлечены в процессы управления рисками.

5.2. Структура управления рисками Общества включает в себя следующие органы и структурные подразделения, перечисленные в пунктах 5.2.1- 5.2.3.

5.2.1. Единоличный исполнительный орган (Генеральный директор Общества, и/или лицо его замещающее).

К компетенции Единоличного исполнительного органа, в части управления рисками, относятся следующие вопросы:

- обеспечение организации системы эффективного управления рисками, позволяющей выявлять, оценивать уровень рисков и управлять ими;
- утверждение внутренних нормативных документов по управлению рисками;
- утверждение перечня мероприятий по управлению существующими рисками;
- распределение полномочий и ответственность по управлению рисками между руководителями структурных подразделений в целях соблюдения основных принципов управления рисками;
- рассмотрение отчетов по результатам деятельности управления рисками;
- принятие решений по осуществлению мероприятий в отношении управления рисками;
- принятие решений по мерам обеспечения непрерывности деятельности Общества в случае реализации чрезвычайной ситуации.

5.2.2. Служба управления рискам (далее – СУР).

К компетенции СУР относятся следующие вопросы:

- разработка методологии и инструментов управления рисками, в том числе в части выявления, оценки, контроля и снижения уровня рисков по всем направлениям деятельности Общества в соответствии с его целями и задачами;
- разработка рекомендаций о мерах, которые необходимо предпринять для устранения (минимизации) того или иного риска, предоставляемых на утверждение Единоличному исполнительному органу Общества;
- разработка рекомендаций о мерах, которые необходимо предпринять для устранения (минимизации) того или иного риска руководителям структурных подразделений;
- определение мер по обеспечению непрерывности деятельности Общества и его операционной надежности;
- оценка уровня рисков с учетом вероятности их наступления и влияния на деятельность Общества;
- осуществление контроля выполнения мер, направленных на устранение (минимизацию) рисков;
- предоставление информации о рисках Единоличному исполнительному органу;
- разработка программ обучения (консультаций) работников по вопросам выявления, идентификации, оценки, контролю, устранению или минимизации рисков;
- осуществление иных функций по управлению рисками, предусмотренных внутренними нормативными документами Общества.

5.2.3. Структурные подразделения, осуществляющие операции.

К компетенции Структурных подразделений Общества относятся следующие вопросы:

- предоставление информации о рисках в части своей компетенции Службе управления рисками для ведения БС ОР;
- осуществление оперативного контроля текущего уровня рисков проводимых операций;
- обеспечение своевременной разработки и реализации мероприятий по управлению рисками;
- принятие оперативных мер по управлению уже реализовавшихся рисков в целях снижения негативных последствий, с выделением ресурсов (в случае необходимости);
- оптимизация бизнес-процессов с целью уменьшения уровня рисков или последствий их реализации;
- учёт информации о рисках при целеполагании и формировании бюджета структурного подразделения;
- интеграция в свои процессы системы управления рисками, в рамках компетенций;
- принятие мер по обеспечению непрерывности деятельности и операционной надежности по процессам своего подразделения, в рамках компетенций;
- обеспечение соблюдения принятых процедур и стратегии управления рисками в рамках своего подразделения;
- участие в процессе постоянного совершенствования системы управления рисками путем формулирования предложений по ее совершенствованию;
- осуществление контроля за операциями и рисками при осуществлении курируемых процессов;
- иные функции, связанные с системой управления рисками, предусмотренные регламентными документами и должностными инструкциями.

6. ПЕРЕЧЕНЬ ОСНОВНЫХ РИСКОВ

6.1. Общество выделяет следующий перечень основных видов рисков: стратегический риск, операционный риск, регуляторный (комплаенс) риск, репутационный риск (риск потери деловой репутации), финансовый риск, санкционный риск.

6.2. Стратегический риск.

Основной целью управления стратегическим риском является минимизация событий и неправильных управленческих решений, которые могут существенно повлиять на деятельность Общества и повлечь за собой убытки.

В целях минимизации стратегического риска Общество предпринимает следующие меры:

- проводит оценку стратегии развития на предмет определения возможности и целесообразности ее реализации, а также внесение изменений в стратегию Общества;
- проводит мероприятия по планированию развития деятельности Общества;
- проводит оценку всех проектов и изменений перед внедрением, с учётом анализа целесообразности;
- проводит анализ эффективности реализованных проектов и изменений по итогам их введения.

6.3. Операционный риск.

Операционному риску подвержены все направления деятельности и процессы Общества, вне зависимости от специфики и объема осуществляемых операций и сделок.

Основной целью управления ОР является минимизация возникновения событий и их последствий, влекущих за собой приостановление или прекращение оказания услуг в полном или неполном объеме, а также риском возникновения убытков Общества.

К отдельным видам ОР, присущим деятельности Общества относятся:

- Риск информационной безопасности (далее - ИБ). Представляет собой риск реализации угроз ИБ, которые обусловлены недостатками процессов обеспечения ИБ, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности Общества.
- Риск информационных систем. Представляет собой риск отказов и (или) нарушения функционирования применяемых Обществом информационных систем.
- Правовой риск. Представляет собой риск возникновения у Общества убытков вследствие: нарушения им и (или) его контрагентами условий заключенных договоров, допускаемых правовых ошибок при осуществлении деятельности, несовершенства правовой системы, нарушения контрагентами нормативных правовых актов, а также контрагентов Общества под юрисдикцией различных государств.
- Проектный риск. Представляет собой риск, состоящий в недостатках и нарушениях организации процессов управления проектной деятельностью.
- Управленческий риск. Представляет собой риск, состоящий в недостатках и нарушениях внутренних процессов Общества, недостатках принятия решений по операциям и внутрихозяйственной деятельности.
- Риск управления персоналом. Представляет собой риск ошибок процесса управления персоналом, состоящий в недостатках и нарушениях внутренних процессов Общества в управлении персоналом, в том числе при подборе, найме, адаптации, увольнении,

обеспечении безопасности и охраны труда, социальной поддержки, в системе вознаграждения и компенсации.

- Риск нарушения непрерывности деятельности. Представляет собой риск нарушения способности Общества поддерживать непрерывность осуществления критически важных процессов, включая нарушения операционной надежности, в результате воздействия источников ОР, в том числе недостатков процессов, действий работников и (или) третьих лиц, от которых зависит выполнение процессов, недостатков систем и оборудования, а также внешних факторов, оказывающих влияние на выполнение процессов Общества.
- Риск аутсорсинга. Представляет собой риск потерь, связанный с ошибками и недостатками организации и осуществления деятельности Общества по передаче своих функций, операций, услуг (или их части) на выполнение (аутсорсинг) третьим лицам (внешним подрядчикам, контрагентам), ненадлежащего исполнения ими переданных им функций, операций, услуг (или их части) на аутсорсинг.

Основными факторами возникновения ОР в деятельности Общества являются:

- недостаточные и (или) неэффективные контрольные процедуры в системах и процессах;
- действия работников, в том числе: ошибки, мошенничество, несоблюдение установленных в Обществе порядков и процедур;
- несовершенство организационной структуры и внутренних документов в части распределения полномочий подразделений и работников, порядков и процедур совершения операций, их документирования и отражения в учете;
- неэффективность внутреннего контроля;
- сбои в функционировании информационных технологий (далее – ИТ) - систем и программно-аппаратных средств;
- внешние обстоятельства, находящиеся вне контроля Общества, включая случаи мошенничества, хакерские атаки, техногенные и природные катастрофы и другие нестандартные или чрезвычайные ситуации.

В Обществе предусмотрены следующие процедуры управления ОР:

- идентификация ОР;
- сбор и регистрация в БСР информации о внутренних событиях ОР и потерях от его реализации;
- определение стоимости потерь и возмещений от реализации событий ОР;
- количественная оценка уровня ОР, определяемая согласно разделу 7 настоящих Правил;
- качественная оценка уровня ОР определяемая экспертным путём с помощью процедуры самооценки рисков;
- выбор и применение способа реагирования на ОР;
- контроль и мониторинг ОР;
- установление порядка предоставления отчетности по вопросам управления ОР.

6.4. Регуляторный (комплаенс) риск.

Общество выделяет следующий перечень регуляторных рисков, подлежащих управлению:

- несоблюдение законодательства Российской Федерации, в том числе требований по ПОД/ФТ/РОМУ, идентификации клиентов, партнёров и контрагентов, защиты их прав и интересов, а также противодействию коррупции;
- несоблюдение внутренних документов и процедур;

- несоблюдение сотрудниками Общества профессиональных стандартов, норм деловой этики и (или) совершение действий, которые могут привести к потере деловой репутации;
- несоответствие внутренних процедур и политик требованиям законодательства/нормативных актов;
- несоответствие внутренних документов фактическим процессам;
- отсутствие внутренних политик;
- претензии/штрафные санкции контролирующих органов;
- риски использования Общества со стороны третьих лиц в целях легализации (отмывания) доходов, полученных преступным путем и финансирования терроризма;
- риски при разработке новых продуктов или расширение в новые сферы бизнеса/новые рынки;
- риски, связанные с внедрением новых технологий;
- риски, связанные, с изменениями в организационной структуре Общества;
- нахождение Потребителей, ФО и контрагентов под юрисдикцией различных государств;
- недобросовестные действия Потребителей/ФО/контрагентов;
- развитие схем внутреннего и внешнего мошенничества, вредительства и ухода от контроля;
- развитие рынка и внедрение новых технологий;
- существенные изменения в экономике и (или) законодательстве (в том числе, иностранном);
- нарушение требований в части идентификации иностранных налогоплательщиков (FATCA/CRS).

Процесс управления регуляторным риском включает в себя:

- идентификацию риска;
- оценку риска;
- выбор и применение способа реагирования на риск, включая разработку перечня мер по снижению риска;
- определение остаточного уровня риска и контроль за выполнением мероприятий по минимизации риска;
- включение информации о выявленных рисках во внутреннюю отчетность по вопросам управления.

Меры по минимизации комплаенс риска могут включать:

- разработку внутренних нормативных документов, регламентирующих процессы и процедуры, связанные с управлением комплаенс-риском;
- автоматизацию контролей;
- обучение сотрудников Оператора ФП.

6.5. Репутационный риск (риск потери деловой репутации).

Основной целью управления репутационным риском является снижения возможных убытков, сохранение и поддержание деловой репутации Общества перед Потребителями, ФО, контрагентами, органами государственной власти.

Основные причины возникновения репутационного риска:

- Освещение негативной информации и (или) дезинформация в СМИ, касающейся деятельности Общества, в том числе технических проблем и (или) реализация иных рисков.
- Жалобы, обращения Потребителей, размещенные на публичных ресурсах без освещения в СМИ.

Общество в рамках управления рисками собирает и анализирует отзывы о своей деятельности в СМИ, включая публикации и отзывы касательно случаев реализации операционных рисков, связанных с техническими проблемами и деятельностью организаций, участвующих в деятельности Общества, в том числе с использованием специализированных автоматизированных информационных систем.

Основные превентивные меры по минимизации репутационного риска:

- Контроль за соблюдением законодательства Российской Федерации, организации внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, законодательства о борьбе с коррупцией.
- Контроль за достоверностью бухгалтерской отчетности.
- Контроль публикуемой информации, в том числе в рекламных целях.
- Мониторинг по различным внешним источникам, путём сбора и анализа информации о деятельности Общества, его партнёрах и контрагентах из:
  - печатных сообщений СМИ: газеты, журналы, другая информация на бумажном носителе;
  - электронной информации в СМИ: телевидение, радио, интернет-источники, в т.ч. социальные сети, информационные каналы, смс–сообщения, сообщения в мессенджерах.

6.6. Финансовый риск.

К основным причинам финансового риска в деятельности Общества относятся:

- риск неуплаты или несвоевременной уплаты комиссионных вознаграждений (при их наличии) со стороны ФО за оказанные услуги, согласно договорам;
- риск финансовых издержек, связанных с деятельностью контрагентов.

В целях минимизации и управления финансовым риском Обществом осуществляется комплекс следующих мер:

- мониторинг финансового положения и оценка уровня кредитного риска по отношению к ФО, с которыми заключены соответствующие договоры;
- оценка финансового положения контрагентов в рамках закупочной деятельности в целях снижения экономических, налоговых, и репутационных рисков.

6.7. Санкционный риск.

Общество выделяет следующие основные источники санкционных рисков, подлежащих управлению:

- риски, связанные с ФО;
- риски, связанные с Потребителями финансовых услуг;
- риски, связанные с контрагентами, в том числе осуществляющими поставку ИТ-оборудования и программного обеспечения, необходимого для функционирования деятельности Общества.

В целях минимизации и управления санкционными рисками по решению Единоличного исполнительного органа может быть сформирован оперативный штаб с подключением в него всех участников, которые могут быть задействованы в управлении рисками.

В качестве мер минимизации могут быть:

- анализ влияния санкций, связанных с Потребителями, ФО и контрагентами на процессы Общества;

- мониторинг санкционных списков;
- проработка мер по минимизации рисков аутсорсинга, включая меры по поиску альтернативных контрагентов;
- другие меры, принятые оперативным штабом.

7. ОПРЕДЕЛЕНИЕ УРОВНЯ ЗНАЧИМОСТИ РИСКОВ

7.1. Критерии уровня значимости рисков определяются исходя из сочетания двух факторов: вероятности (частоты) возникновения события риска и влияния данного события на деятельность Общества (потенциального или фактического).

7.2. Все описанные критерии значимости рисков применимы к операционным рискам. Для остальных видов рисков, описанных в разделе 6, критерии (факторы вероятности) для определения уровня значимости риска используются в рамках применимости. В случае неприменимости описанных критериев, уровень значимости рисков может определяться экспертным путём уполномоченными лицами, назначенными Единым исполнительным органом, либо в рамках деятельности оперативного штаба.

7.3. Для определения уровня значимости используется Матрица уровня значимости, приведённая в Таблице 1. «Матрица уровня значимости рисков».

Таблица 1. «Матрица уровня значимости рисков»:

Матрица уровня значимости			Влияние			
			Низкое	Среднее	Высокое	Очень высокое
			1	2	3	4
Вероятность	Очень высокая	4	Средний	Высокий	Очень высокий	Очень высокий
	Высокая	3	Средний	Средний	Высокий	Очень высокий
	Средняя	2	Низкий	Средний	Высокий	Высокий
	Низкая	1	Низкий	Низкий	Средний	Высокий

1) Вероятность (частота) возникновения события риска

Вероятность (частота) события		**Количество событий**
Очень высокая	4	от 20 раз в год
Высокая	3	от 10 до 20 раз в год
Средняя	2	от 4 до 10 раз в год
Низкая	1	до 3-х раз в год

2) Влияние от реализации свершившегося риска

Финансовое влияние:

Влияние		Сумма финансовых влияний (руб. за 1 событие)
Очень высокое	4	≥ 20 000 000
Высокое	3	≥ 1 000 000 и < 20 000 000
Среднее	2	≥ 100 000 и < 1 000 000
Низкое	1	< 100 000

Нефинансовое влияние.
Нефинансовое влияние может оцениваться в части: регуляторного влияния, репутационного влияния, процессного влияния.

Регуляторное влияние:

Влияние		Описание
Очень высокое	4	Предупредительные меры воздействия/принудительные меры воздействия со стороны контролирующих и регулирующих органов власти в виде потенциального штрафа свыше 20 млн. руб. Риск отзыва лицензии.
Высокое	3	Предупредительные меры воздействия/принудительные меры воздействия со стороны контролирующих и регулирующих органов власти в виде потенциального штрафа до 20 млн. руб.
Среднее	2	Предупредительные меры воздействия/принудительные меры воздействия со стороны контролирующих и регулирующих органов власти в виде потенциального штрафа до 1 млн. руб.
Низкое	1	Несоответствия деятельности сложившейся практике, выявленные подразделениями Общества/консультантами/аудиторами по заказу Общества.

Влияние на репутацию Общества:

Влияние		Описание
Очень высокое	4	Освещение/дезинформация в СМИ/официальные заявления со стороны Банка России следующей информации: • Общество не выполняет свои обязательства перед Потребителями/ФО; • предположение о предстоящем отзыве лицензии/приостановлении деятельности/принудительном ограничении деятельности по отдельным видам операций.
Высокое	3	Жалобы/обращения Потребителей, размещенные на публичных ресурсах без освещения в СМИ. Освещение негативной информации/дезинформация в СМИ/официальные заявления со стороны Банка России в адрес основных партнёров Общества.
Среднее	2	Жалобы/обращения Потребителей, размещенные на публичных ресурсах без освещения в СМИ.
Низкое	1	Жалобы/обращения Потребителей, поступившие по внутренним каналам связи и необоснованные жалобы в адрес Общества и другие надзорные органы.

Влияние на процессы Общества:

Влияние		Описание
Очень высокое	4	Подразделения Общества не способны выполнять свои основные функции. Приостановлено функционирование более одного критически важного процесса на период, превышающий 24 часа.
Высокое	3	Прерывание/остановка деятельности критически-важных процессов на период от 2 часов до 24 часов.

Среднее	2	Прерывание/остановка деятельности критически-важных процессов на период до 2 часов.
Низкое	1	Затронутые процессы могут продолжать свою деятельность, с увеличенным техническим интервалом обслуживания.

8. УПРАВЛЕНИЕ РИСКАМИ, СПОСОБЫ РЕАГИРОВАНИЯ И ПЕРЕЧЕНЬ МЕР

8.1. СУР, совместно со структурными подразделениями Общества применяет превентивные меры по выявлению возможных потенциальных рисков, с помощью:

- проведение качественной оценки, включая самооценку рисков (в том числе экспертную) структурными подразделениями Общества;
- проведение количественной оценки рисков.

8.2. По итогам определения уровня рисков, с учётом качественной и количественной оценки, СУР, совместно с ответственными структурными подразделениями Общества определяет оптимальный способ реагирования на риски. Основные способы реагирования на риски:

- уклонение (отказ) от риска – отказ Общества от оказания соответствующего вида услуг и операций в связи с высоким уровнем ОР в них;
- передача риска – страхование, передача Обществом риска другой стороне – контрагенту и (или) иной третьей стороне на основании договора;
- принятие риска – готовность Общества понести возможные потери, в рамках установленного лимита потерь (для принятия рисков решение выносится на утверждение со стороны Единоличного исполнительного органа);
- принятие мер минимизации, включая разработку форм (способов) контроля с учетом оценки их эффективности и уровня остаточного риска.

8.3. Перечень рекомендуемых возможных мер, направленных на уменьшение негативного влияния рисков, которым могут руководствоваться структурные подразделения Общества в рамках системы управления рисками, но не ограничиваться им:

- регламентация, в том числе актуализация, процессов проведения операций (сделок) с соблюдением действующего законодательства;
- применение стандартизированных форм внутренних документов Общества;
- стандартизация операций (сделок);
- применение стандартизированных форм договоров с клиентами (контрагентами);
- контроль (автоматизированный, ручной) за соблюдением внутренних документов Общества;
- подбор и аттестация персонала;
- разработка системы мотивации персонала;
- проведение тренингов и обучение персонала проведению операций;
- процедура коллегиального принятия решений, например, по проведению нестандартных операций;
- особый контроль за проведением нестандартных операций;
- контроль операций;
- формирование отчетов по операциям (с учетом требований регулятора);

- тестирование процессов, информационных и технологических систем;
- автоматизация процессов;
- проверка документов, в том числе первичных, по проводимым сделкам с контрагентами;
- разграничение функций, ответственности и полномочий персонала операций;
- использование двойного контроля при проведении операций;
- установление и контроль соблюдения лимитов при проведении операций;
- установление и разделение прав доступа к информации и информационным системам;
- резервирование информации в информационных системах;
- установление и разделение прав доступа к использованию материальных и нематериальных активов;
- организация физической безопасности объектов и материальных активов Общества;
- противодействие неправомерному использованию инсайдерской информации;
- контроль качества данных в процессах, информационных системах;
- процедуры ограничения на ввод данных в информационных системах;
- автоматический контроль вводимых данных в информационных системах;
- контроль сроков и рассылка уведомлений участникам процессов;
- автоматический контроль маршрута операций;
- мероприятия по повышению культуры управления рисками;
- система ключевых показателей деятельности, стимулирующая персонал эффективно управлять рисками;
- другие меры, направленные на уменьшение негативного влияния рисков.

Приведённый перечень мер носит рекомендательный характер, и может быть использован в случае применимости.

9. НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ И ОПЕРАЦИОННАЯ НАДЁЖНОСТЬ

9.1. В части обеспечения непрерывности и (или) восстановления деятельности в случае нестандартных и чрезвычайных ситуаций Общество разрабатывает и утверждает:

- План обеспечения непрерывности и (или) восстановления деятельности Акционерного общества «Универсальные Финансовые Технологии» в случае возникновения нестандартных и чрезвычайных ситуаций (далее - План ОНиВД).
- Программу непрерывности деятельности Акционерного общества «Универсальные Финансовые Технологии».

9.2. Документы, описанные в п.9.1 определяют:

- основные принципы и методы обеспечения непрерывности деятельности Общества при возникновении нестандартных и чрезвычайных ситуаций;
- устанавливают цели, задачи, порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования процессов Общества;
- определяют перечень возможных сценариев нарушения непрерывности деятельности и перечень наиболее возможных нестандартных и чрезвычайных ситуаций.

9.3. Обеспечение непрерывности деятельности Общества реализуется на основе:

- вовлеченности сотрудников Общества в процесс обеспечения непрерывности деятельности, за счет их обучения, осведомленности о целях Общества в области обеспечения непрерывности деятельности;
- ознакомления сотрудников Общества с Планом ОНиВД Общества и осознании важности его соблюдения;
- непрерывного улучшения и совершенствования процессов ОНиВД, а также привлечения сотрудников Общества к процессам обеспечения непрерывности деятельности Общества.

9.4. Внутренними документами Общества, в том числе документами в части ОНиВД и документами по информационной безопасности, устанавливаются требования к операционной надежности, включающие:

- определение пороговых значений допустимого времени простоя и (или) деградации технологических процессов;
- комплекс мер, направленный на поддержание непрерывности оказания финансовых услуг, который включает в себя:
    - разработку и внедрение целевых значений показателей операционной надежности;
    - проведение категорирования и обеспечение безопасности критической информационной инфраструктуры, в т.ч. при процессах управления изменениями критичной архитектуры;
    - выявление, регистрацию, реагирование на инциденты операционной надежности, в т.ч. организацию восстановления технологических процессов по факту возникновения инцидентов;
    - обеспечение выполнения требований по операционной надежности при взаимодействии с поставщиками услуг Общества;
    - тестирование операционной надежности технологических процессов Общества;
    - информирование заинтересованных сторон о возникших инцидентах операционной надежности.

9.5. Структурными подразделениями Общества, совместно с СУР проводится процедура самооценки процессов обеспечения непрерывности деятельности и готовности к инцидентам, определяемая экспертным путём.

9.6. Результаты самооценки, а также отчеты содержащие результаты тестирования Плана ОНиВД, включая тестирование программно-технических средств и (или) ИТ-инфраструктуры выносятся на утверждение Единоличному исполнительному органу.

9.7. Периодичность и сроки проведения самооценки и отчетности определяются отдельными внутренними распорядительными документами, утвержденными Единым исполнительным органом.

10. ОПЕРАЦИИ БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ ПОТРЕБИТЕЛЕЙ (КЛИЕНТОВ)

10.1. Общество устанавливает требования к операционной надежности, порядку и срокам хранения и защиты информации при осуществлении деятельности по функционированию Платформы. Соблюдение указанных требований обеспечивает реализацию мероприятий по выявлению операций, направленных на совершение финансовых сделок без волеизъявления Потребителей и ФО, и противодействию в совершении незаконных финансовых сделок.

10.2. Общество устанавливает требования к безопасности процессов Платформы комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации.

10.3. Общество на постоянной основе осуществляет выявление операций по финансовым сделкам без волеизъявления Потребителей, в том числе совершенные в результате несанкционированного доступа к информационным системам Общества.

10.4. В целях контроля, а также предотвращения операций без волеизъявления Потребителей, Общество применяет полученную от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления операций по финансовым сделкам без волеизъявления Потребителей.

10.5. Общество направляет в Банк России информацию обо всех случаях и (или) о попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, по форме и в порядке, которые установлены Банком России.

10.6. Общество осуществляет реализацию мероприятий по выявлению атак на объекты ИТ-инфраструктуры Общества и (или) Потребителей, которые могут привести к случаям и (или) попыткам осуществления операций по финансовым сделкам без волеизъявления Потребителей.

10.7. Общество осуществляет сбор технических данных, описывающих компьютерные атаки, направленные на объекты своей ИТ инфраструктуры, Потребителей, а также сбор сведений об обращении Потребителей в правоохранительные органы, при их наличии.

10.8. Общество предоставляет условия для направления Потребителями уведомлений о совершении финансовых сделок без их волеизъявления, а также обеспечивает учет, регистрацию и хранение указанных уведомлений. Согласно Правилам финансовой платформы: Потребитель обязан немедленно уведомить Оператора финансовой платформы по любому из доступных ему предусмотренных Оператором финансовой платформы каналах связи о любом случае и (или) о попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления Потребителя.

10.9. Общество применяет все доступные меры защиты информации, а также вводит ограничения по параметрам операций по финансовым сделкам, устанавливаемых на основании заявления Потребителей.

10.10. Общество в рамках реализуемых им процессов управления рисками вправе отказать в оказании услуги по обеспечению удаленного взаимодействия Потребителей с ФО для совершения финансовых сделок, или принять решение о приостановлении допуска к совершению финансовых сделок при наступлении случая и (или) попытки осуществления операций, направленных на совершение финансовых сделок с использованием Платформы без волеизъявления Потребителя.

10.11. Вся информация о событиях выявления операций по финансовым сделкам без волеизъявления Клиентов, в том числе совершенных в результате несанкционированного доступа к информационным системам Общества, подлежит фиксации в БСР и направляется в СУР.

10.12. Ответственность за мониторинг операций, мероприятия устранению и (или) минимизации операций без волеизлияния Потребителей, перечисленных в настоящем разделе возлагается на структурные подразделения, согласно их компетенций, на основании возложенных на них обязанностей в соответствии с внутренними регламентными документами и должностными инструкциями.

11. ОТЧЕТНОСТЬ

11.1. Отчетность формируется в соответствии с требованиями внутренних нормативных документов Общества, регламентирующих управление тем или иным видом рисков, требованиями Банка России и требованиям к раскрытию информации по рискам для всех заинтересованных сторон.

11.2. Сбор данных о событиях реализовавшихся рисков и формирование отчётности по рискам осуществляет СУР.

11.3. Отчёт о значимых рисках, с перечнем мероприятий по управлению существующими рисками утверждается Единоличным исполнительным органом.

11.4. Отчётность по рискам осуществляется в соответствии со следующими принципами:
точность и информативность, своевременность, полнота данных.

12. РАСКРЫТИЕ ИНФОРМАЦИИ

12.1. Общество доводит до акционеров, потребителей, финансовых организаций, а также регулирующих органов, внешних аудиторов и других заинтересованных лиц информацию о действующей системе управления рисками Общества.

12.2. Раскрытие информации осуществляется в следующих объемах:

- для акционеров – краткая характеристика процессов управления рисками (а также иная информация, доводимая в соответствии с требованиями регулирующих органов или внутренними документами);
- для регулирующих органов - с периодичностью и в объеме, установленном соответствующими нормативными документами;
- для внешних аудиторов, регулирующих органов в ходе проведения проверок - на основании распоряжения органов управления.

12.3. Механизмами раскрытия информации являются:

- размещение информации на сайте Общества в информационно-телекоммуникационной сети «Интернет»;
- предоставление отчетности, обозначенной во внутренних нормативных документах и регуляторных требованиях по управлению рисками.

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Настоящие Правила вступают в силу с даты их утверждения Решением единственного акционера Общества и действуют до утверждения новой редакции Правил.

13.2. Пересмотр и обновление настоящих Правил осуществляется не реже 1 раза в 2 (два) года.

13.3. Настоящие Правила хранятся в бумажном виде в СУР. Электронная копия Правил хранится в электронной базе документов Общества.

ИЗМЕНЕНИЯ

Номер редакции	Дата изменений	Описание изменений
1	05.09.2023	Документ введен впервые.