

Закрытое акционерное общество
"Уайт Бёрд"



ПОЛОЖЕНИЕ
23.07.2024 №

г. Минск

О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ

Глава 1 ОБЩИЕ ПОЛОЖЕНИЯ

1. Положение о системе управления рисками (далее – Положение) и определяет цели, задачи, принципы и методы управления рисками, а также организацию системы управления рисками в ЗАО "Уайт Бёрд" (далее – Общество).

2. Исходя из своей профессиональной деятельности в качестве оператора криптовалюты, Общество выделяет для себя следующие основные виды рисков:

- **Кредитный риск** – риск возникновения у Общества потерь (убытков), неполучения запланированных доходов вследствие неисполнения или ненадлежащего исполнения должником финансовых и иных имущественных обязательств перед Обществом в соответствии с условиями договора или законодательством;

- **Страновой риск** – риск возникновения у Общества потерь (убытков), неполучения запланированных доходов в результате неисполнения или ненадлежащего исполнения иностранными контрагентами (юридическими, физическими лицами) обязательств из-за экономических, политических, социальных изменений, а также вследствие того, что валюта денежного обязательства может быть недоступна контрагенту из-за особенностей законодательства (независимо от финансового положения самого контрагента);

- **Рыночный риск** – риск возникновения у Общества потерь (убытков), неполучения запланированных доходов в результате волатильности на рынках токенов и иных финансовых рынках;

- **Риск ликвидности** – вероятность возникновения у Общества потерь (убытков), неполучения запланированных доходов вследствие неспособности обеспечить исполнение своих обязательств своевременно и в полном объеме;

- **Операционный риск** – риск возникновения у Общества потерь (убытков) и (или) дополнительных затрат в результате несоответствия установленных Обществом порядков и процедур совершения и (или) исполнения сделок (операций) с токенами и иных сделок (операций) законодательству, актам Наблюдательного совета ПВТ или их нарушения работниками Общества, некомпетентности или ошибок работников Общества, несоответствия или отказа используемых Обществом систем, в том числе

информационных, а также в результате действия внешних факторов, включая осуществление Обществом аутсорсинга. Одними из основных видов операционного риска также являются правовой риск и кибер-риск, которые в том числе могут возникать в сочетании с иными видами операционного риска;

- **Правовой риск** – риск возникновения у Общества потерь (убытков) и (или) дополнительных затрат вследствие допускаемых правовых ошибок при осуществлении деятельности, противоречивости, несовершенства и изменчивости законодательства, а также в результате судебных процессов, других правовых процедур, оказывающих негативное воздействие на деятельность Общества;

- **Кибер-риск** – риск возникновения у Общества потерь (убытков) и (или) дополнительных затрат вследствие противоправных действий сторонних лиц в отношении компьютерных и информационных систем или сетей, систем связи, информационных ресурсов и потоков Общества, совершаемых посредством информационных и телекоммуникационных технологий. Кибер-риск возникает вследствие воздействия на компьютерные и информационные системы или сети, системы связи, информационные ресурсы и потоки Общества с целью получения несанкционированного доступа к информации, обрабатываемой и (или) хранящейся в информационной системе Общества, и информационным потокам (угроза информационной безопасности), нарушения функционирования информационной системы и (или) системы защиты информации, осуществляемого посредством внедрения вредоносного программного обеспечения либо иных деструктивных воздействий, источником которых являются глобальная компьютерная сеть Интернет или другие внешние информационные сети и системы;

- **Риск потери деловой репутации (репутационный риск)** – риск возникновения у Общества потерь (убытков), неполучения запланированных доходов в результате сужения клиентской базы, снижения иных показателей развития вследствие формирования в обществе негативного представления о финансовой надежности Общества, качестве оказываемых услуг или характере деятельности в целом. Репутационный риск Общества может возникнуть из-за недостатков в организации деятельности, сбоев в работе электронных систем Общества, несоблюдения законодательства, локальных нормативных правовых актов Общества, отступления от обычая делового партнерства, подозрения в участии Общества или его сотрудников в незаконных финансовых операциях, в легализации доходов, полученных преступным путем, финансировании террористической деятельности и финансировании распространения оружия массового поражения, а также в иной противоправной деятельности;

- **Риск концентрации** – риск возникновения у Общества потерь (убытков), неполучения запланированных доходов в результате концентрации отдельных видов рисков;

- **Риск, связанными с легализацией доходов**, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения.

3. Указанные выше виды рисков не является исчерпывающим и могут дополняться вновь выявленными существенными рисками.

Глава 2

ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

4. Цели системы управления рисками (СУР):

- заблаговременное выявление уязвимостей и угроз в деятельности Общества;
- ограничение потенциальной возможности реализации рисков Общества;
- оперативное реагирование на внешние и внутренние изменения и предотвращение последствий возможных неблагоприятных событий.

5. Задачи СУР:

- своевременное выявление и управление наиболее существенными рисками, влияющими на стратегические цели Общества и способными причинить существенный негативный ущерб или привести к приостановке деятельности Общества;
- обеспечение разумной уверенности в достижении целей Общества;
- обеспечение эффективности финансово-хозяйственной деятельности и экономичного использования финансовых ресурсов Общества;
- обеспечение сохранности активов Общества;
- предотвращение реализации рисков и снижение их последствий до максимально возможного уровня;
- обеспечение роста доверия Клиентов и укрепление положительной репутации Общества;

6. СУР основывается на следующих принципах:

- управление рисками осуществляется непрерывно и на систематической основе;
- деятельность по управлению рисками носит превентивный характер и направлена на снижение вероятности и/или ущерба от реализации рисков, а не на устранение последствий такой реализации;
- для управления рисками используется максимально точная, полная и достоверная информация, включая информацию за прошедшие периоды, аналитические материалы, прогнозы и др.

Глава 3

УЧАСТНИКИ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ И ИХ ФУНКЦИИ

7. Структура СУР в Обществе включает вовлечение следующих лиц:

- руководитель Общества;
- должностное лицо Общества, ответственное за организацию управления рисками;

- руководители структурных подразделений Общества;
- прочие работники Общества.

8. Руководитель Общества отвечает за организацию эффективной СУР, позволяющей выявлять, оценивать и управлять рисками Общества, в том числе:

- распределяет полномочия в сфере управления рисками между подразделениями, отдельными работниками, в том числе назначает должностное лицо Общества, ответственное за организацию управления рисками (далее - ОДЛ);
- использует информацию о рисках, предоставленную ОДЛ, при принятии управленческих решений.

9. Должностное лицо Общества, ответственное за организацию управления рисками:

- подчиняется непосредственно руководителю Общества;
- выявляет риски, возникающих при осуществлении Обществом деятельности оператора криптовалюты;
- выявляет источники возникновения рисков;
- осуществляет управление рисками с учетом их существенности;
- координирует и контролирует работу структурных подразделений и работников по вопросам управления рисками;
- участвует в разработке и внедрении методик выявления, оценки и контроля рисков, в разработке мероприятий по управлению рисками;
- участвует в расследовании случаев реализации рисков;
- осуществляет сбор необходимой информации в рамках своей компетенции для её незамедлительного предоставления руководителю Общества.

10. Руководители структурных подразделений Общества:

- обеспечивают соблюдение положений внутренних документов Общества, регулирующих вопросы управления рисками, работниками своих структурных подразделений;
- оказывают содействие ОДЛ в выполнении им своих обязанностей;
- представляют ОДЛ информацию о рисках в области своей компетенции;
- оптимизируют бизнес-процессы с целью уменьшения уровня рисков или последствий их реализации.

11. Прочие работники Общества:

- реализуют утвержденные мероприятия по управлению рисками;
- осуществляют мониторинг уровня рисков в области своей компетенции.

Глава 4

ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ

12. Идентификация рисков. Идентификация рисков – процесс выявления рисков и их основных источников, обнаружения событий, источников их возникновения и возможных последствий, исследования и описания рисков.

Для идентификации риска могут использоваться данные прошлых лет (иных периодов времени), теоретический анализ, мотивированные экспертные суждения и осведомленность о соответствующих факторах.

13. Оценка рисков. Оценка рисков – процесс определения уровня риска путем присвоения каждому риску величины возможного ущерба и вероятности наступления такого ущерба с целью дальнейшей разработки мероприятий по управлению риском.

Оценка риска предусматривает процесс сравнения результатов измерения риска с установленными критериями риска для определения приемлемости (допустимости) риска и (или) его величины. Для оценки рисков применяется следующая матрица:

		Значимость		
		Высокая	Средняя	Низкая
Вероятность	Высокая	5	4	2
	Средняя	4	3	1
	Низкая	3	2	1
5-4 – Опасный уровень риска				
3-1 – Допустимый уровень риска				

Оценка риска включает сравнение уровня риска, выявленного в процессе измерения, и критериев риска, на основании которого определяется дальнейшее отношение к риску.

13.1. В отношении предусмотренных настоящим Положением рисков применяются два уровня оценки опасности риска:

- опасный уровень риска;
- допустимый уровень риска.

13.2. Оценка уровня риска устанавливается по совокупности оценок значимости риска и вероятности реализации риска;

13.3. Значимость риска – характеристика степени возможного ущерба от наступления рискового события оценивается по шкале:

- высокая значимость;
- средняя значимость;
- низкая значимость.

13.4. Вероятность реализации риска – вероятность наступления рискового события, приносящего ущерб, оценивается по шкале:

- высокая вероятность;
- средняя вероятность;
- низкая вероятность.

13.5. Опасный (недопустимый) уровень риска – соответствующий одновременно:

- высокой степени значимости и высокой степени вероятности реализации (оценка опасности риска - 5 баллов);
- высокой степени значимости и средней степени вероятности реализации (оценка опасности риска - 4 балла);
- средней степени значимости и высокой степени вероятности реализации(оценка опасности риска - 4 балла).

13.6. Допустимый уровень риска – соответствующий одновременно:

- высокой степени значимости и низкой степени вероятности реализации(оценка опасности риска - 3 балла);
- средней степени значимости и средней степени вероятности реализации(оценка опасности риска - 3 балла);
- средней степени значимости и низкой степени вероятности реализации(оценка опасности риска - 2 балла);
- низкой степени значимости и высокой степени вероятности реализации(оценка опасности риска - 2 балла);
- низкой степени значимости и средней степени вероятности реализации (оценка опасности риска - 1 балл);
- низкой степени значимости и низкой степени вероятности реализации (оценка опасности риска - 1 балл).

13.7. Опасный уровень риска может быть снижен до допустимого уровня риска в результате принятия Обществом мер по минимизации риска.

14. Реагирование на риски. Реагирование на риск предусматривает принятие мер по результатам выявления (идентификации) и измерения (оценки) риска.

Выбор способов реагирования на риск производится путем сравнения их эффективности с целью минимизации возможного ущерба в будущем. Способами реагирования на риск являются:

- уклонение от риска посредством отказа от начала либо продолжения деятельности, в результате которой возникает риск;
- сохранение риска (принятие риска либо при необходимости его изменения до величины, не превышающей допустимого уровня);
- ограничение (снижение) риска (уменьшение вероятности возникновения риска и (или) размеров возможного ущерба при наступлении неблагоприятных событий);
- передача риска (разделение риска с другой стороной или его передача другой стороне (аутсорсинг).

15. В случае произшествия факта реализации риска Общество совершает следующие действия:

- определение причин, повлекших факт реализации риска;
- устранение последствий факта реализации риска (если это возможно);
- принятие мер по недопущению произшествия аналогичного (сходного) факта реализации риска в будущем.

16. Контроль рисков. Контроль рисков состоит из комплекса мер, подразумевающих осуществление:

- предварительного контроля – путем подбора квалифицированных кадров; разработки четких, детальных и недвусмысленных должностных инструкций, исключающих возникновение конфликта интересов, порядков осуществления операций; предварительного анализа рискованности и эффективности проводимых операций; обеспечения Общества необходимыми техническими средствами, оборудованием, информационными технологиями;
- текущего контроля – путем проверки соблюдения требований законодательства Республики Беларусь, локальных нормативных правовых актов Общества по управлению рисками, установленных процедур принятия соответствующих решений, осуществления операций с криптовалютой, иных финансовых операций;
- последующего контроля – путем проверки обоснованности и правильности совершения операций, соответствия выполняемых работниками функций должностным инструкциям; сопоставления понесенных и планируемых (прогнозных, смоделированных) потерь, сопоставления плановых и фактических показателей деятельности.

17. Мониторинг рисков. Мониторинг рисков – систематическое обновление информации об уровне риска и внешних или внутренних

факторах, влияющих на уровень риска, а также о статусе мероприятий по управлению риском. В рамках мониторинга рисков:

- идентифицируются новые риски;
- пересматривается оценка уровня риска;
- рассматривается статус внедрения и эффективность мероприятий по управлению рисками. При необходимости разрабатываются дополнительные мероприятия по управлению рисками.

Глава 5 ПРОЧИЕ ПОЛОЖЕНИЯ

18. При раскрытии информации о системе управления рисками Общество руководствуется принципом открытости, но при этом обеспечивает соблюдение установленного законодательством Республики Беларусь порядка представления информации, составляющей коммерческую или иную охраняемую законом тайну и другую конфиденциальную информацию.

19. Настоящее Положение подлежит по крайней мере ежегодному пересмотру с целью его поддержания в состоянии, обеспечивающем возможность полного выполнения задач системы управления рисками Общества.

ЛИСТ
ознакомления работников ЗАО “Уайт Бёрд”
с положением о системе управления рисками