Об утверждении Правил формирования системы управления рисками и внутреннего контроля для операторов обмена необеспеченных цифровых активов, операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов

Постановление Правления Национального Банка Республики Казахстан от 29 апреля 2026 года № 47. Зарегистрировано в Министерстве юстиции Республики Казахстан 30 апреля 2026 года № 38614

Примечание ИЗПИ!

Введение в действие см. п.4.

В соответствии с подпунктом 10) части второй пункта 1 статьи 4 Закона Республики Казахстан "О цифровых активах в Республике Казахстан" Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые Правила формирования системы управления рисками и внутреннего контроля для операторов обмена необеспеченных цифровых активов, операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов (далее – Правила).

2. Департаменту платежных систем и цифровых финансовых технологий Национального Банка Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом Национального Банка Республики Казахстан государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Национального Банка Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент Национального Банка Республики Казахстан сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Национального Банка Республики Казахстан.

4. Настоящее постановление вводится в действие с 1 мая 2026 года и подлежит официальному опубликованию.

Приостановить до 12 июля 2026 года действие:

подпунктов 1), 8) и 27) пункта 2 Правил, установив, что в период приостановления данные подпункты действуют в следующей редакции:

"1) информационный актив – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;

8) риск информационной безопасности – вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов ПУЦА;

27) риск информационных технологий – вероятность возникновения ущерба вследствие отказа (нарушения функционирования) информационно-коммуникационных технологий, эксплуатируемых ПУЦА;";

подпункта 16) пункта 2 Правил, установив, что в период приостановления данный подпункт действует в следующей редакции:

"16) операционный риск – риск возникновения расходов (убытков) в результате недостатков или ошибок в ходе осуществления внутренних процессов, допущенных со стороны работников (человеческих ресурсов) и ходе ненадлежащего функционирования информационных систем, цифровых платформ (торговых платформ) и технологий, а также вследствие влияния внешних событий, за исключением стратегического риска и репутационного риска;";

подпункта 24) пункта 2 Правил, установив, что в период приостановления данный подпункт действует в следующей редакции:

"24) система управления рисками – совокупность взаимосвязанных элементов: процедур, методик, информационных систем, объединенных в единый процесс по управлению реализованными и потенциальными рисками в рамках приемлемого для акционера (участника) уровня риска и направленных на достижение целей и задач по управлению рисками. В процессе выявления и управления реализованными и потенциальными рисками, влияющими на деятельность ПУЦА, участвуют органы ПУЦА, руководящие работники и работники структурных подразделений (ответственные работники) в пределах закрепленной компетенции и ответственности. Процесс выявления и управления реализованными и потенциальными рисками включает в себя оценку риска, измерение риска, контроль риска и мониторинг риска;";

подпункта 1) пункта 3 Правил, установив, что в период приостановления данный подпункт действует в следующей редакции:

"1) эффективного управления рисками ПУЦА посредством своевременного их выявления, измерения, контроля и мониторинга для обеспечения соответствия деятельности ПУЦА, выбранной бизнес модели, требованиям по корпоративному управлению, функционированию информационных систем, цифровых платформ (торговых платформ) и систем управленческой информации, проведению разрешенных операций, управлению активами и обязательствами, функционированию системы учета ПУЦА и иных информационных и коммуникационных систем ПУЦА, а также уровню принимаемых им рисков и наличия соответствующего уровня ликвидности;";

подпунктов 3), 4) и 5) пункта 7 Правил, установив, что в период приостановления данные подпункты действуют в следующей редакции:

"3) проведение регулярного мониторинга систем учета, иных информационных и коммуникационных систем (цифровых платформ, торговых платформ) в целях обеспечения бесперебойности, непрерывности деятельности процесса оказания услуг цифровых активов для ПУЦА (за исключением оператора обмена необеспеченных цифровых активов), учета прав по цифровым активам и иным финансовым инструментам, расчетов в цифровых активов и (или) деньгах, а также отражения сведений, содержащихся в соответствующих системах учета;

4) проведение ежегодного внутреннего аудита программно-технического обеспечения ПУЦА, включая информационные и коммуникационные системы, используемые ПУЦА в своей деятельности;

5) разработка и реализация проектов, направленных на дальнейшее развитие и совершенствование деятельности ПУЦА в части функционирования систем учета, информационных и коммуникационных систем (цифровых платформ, торговых платформ), процесса оказания услуг цифровых активов для ПУЦА, учета ПУЦА (за исключением оператора обмена необеспеченных цифровых активов) прав по цифровым активам, расчетов в цифровых активах, отражения сведений, содержащихся в системах учета, автоматизации отдельных операций, совершаемых в ПУЦА, а также процесса сбора, ввода, учета, хранения информации и иных направлений деятельности ПУЦА;";

подпункта 2) пункта 34 Правил, установив, что в период приостановления данный подпункт действует в следующей редакции:

"2) недоступность технологий, в том числе информационных и коммуникационных технологий (компьютерные вирусы, отказ компьютерных аппаратных средств, потеря связи);";

подпункта 2) пункта 42 Правил, установив, что в период приостановления данный подпункт действует в следующей редакции:

"2) неэффективными стратегиями, политиками и (или) стандартами в области информационных технологий, недостатками в использовании программного обеспечения;";

подпункта 12) пункта 42 Правил, установив, что в период приостановления данный подпункт действует в следующей редакции:

"12) вероятностью возникновения ошибок и сбоев в функционировании программно-технического обеспечения ПУЦА, включая соответствующие системы учета, а также в эксплуатируемых информационных и коммуникационных системах и технологиях;";

глав 10 и 11 Правил, установив, что в период приостановления данные главы действуют в следующей редакции:

"Глава 10. Управление рисками информационных технологий

44. Система управления рисками информационных технологий включает, но не ограничивается:

1) политику управления рисками информационных технологий;

2) процедуры управления рисками информационных технологий;

3) систему управленческой информации;

4) оценку эффективности системы управления рисками информационных технологий подразделением внутреннего аудита (ответственным работником по внутреннему аудиту).

45. ПУЦА определяет следующих участников системы управления рисками информационных технологий (но не ограничиваясь ими):

1) подразделение (ответственный работник) по управлению рисками ПУЦА;

2) подразделение (ответственный работник) по информационным технологиям.

46. ПУЦА создает структурное подразделение (назначает ответственного работника) по управлению рисками, в функции которого входит управление рисками информационных технологий, включая:

1) разработку, внедрение и развитие системы управления рисками информационных технологий;

2) участие в разработке и согласовании планов мероприятий по реализации стратегии ПУЦА в части обеспечения доступности информационно-коммуникационных технологий;

3) участие в оценке рисков информационных технологий;

4) мониторинг уровня рисков информационных технологий;

5) взаимодействие и консультирование структурных подразделений (ответственного работника) ПУЦА по вопросам управления рисками информационных технологий;

6) планирование проведения и анализ результатов оценки рисков информационных технологий, проводимой подразделением (ответственным работником) по информационным технологиям;

7) разработка и формирование реестра рисков, включающего риски информационных технологий;

8) предоставление отчетности о реализации существенных рисков информационных технологий и мониторинг исполнения мероприятий по устранению их последствий органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

9) предоставление отчетности или иной информации по управлению рисками информационных технологий органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

10) использование результатов внутреннего аудита в части рисков информационных технологий.

47. ПУЦА создает структурное подразделение (назначает ответственного работника) по информационным технологиям, в функции которого входит:

1) проведение оценки рисков информационных технологий;

2) разработка мер по обработке рисков информационных технологий и предоставление отчетности по их реализации в подразделение по управлению рисками;

3) подготовка и предоставление отчетности о реализации существенных рисков информационных технологий в подразделение рисков ПУЦА, а также об устранении их последствий;

4) разработка планов мероприятий по реализации стратегии ПУЦА в части обеспечения доступности информационно-коммуникационных технологий для критичных бизнес-процессов.

Глава 11. Управление рисками информационной безопасности

48. Система управления рисками информационной безопасности включает, но не ограничивается:

1) политику управления рисками информационной безопасности;

2) процедуры управления рисками информационной безопасности;

3) систему управленческой информации;

4) оценку эффективности системы управления рисками информационной безопасности подразделением внутреннего аудита (ответственным работником по внутреннему аудиту).

49. ПУЦА определяет следующих участников системы управления рисками информационной безопасности (но не ограничиваясь ими):

1) подразделение (ответственный работник) по управлению рисками ПУЦА;

2) подразделение (ответственный работник) по информационной безопасности;

3) подразделение (ответственный работник) по информационным технологиям;

4) подразделения-владельцы защищаемой информации.

50. ПУЦА создает структурное подразделение (назначает ответственного работника) по управлению рисками, в функции которого входит управление рисками информационной безопасности:

1) разработка, внедрение и развитие системы управления рисками информационной безопасности;

2) участие в разработке и согласовании планов мероприятий по реализации стратегии ПУЦА в части обеспечения информационной безопасности;

3) создание и руководство рабочей группой по формированию перечня критичных информационных активов ПУЦА, включающей как минимум подразделения-владельцев защищаемой информации;

4) участие в оценке рисков информационной безопасности;

5) мониторинг уровня рисков информационной безопасности;

6) взаимодействие и консультирование структурных подразделения ПУЦА (ответственного работника) по вопросам управления рисками информационной безопасности;

7) планирование проведения и анализ результатов оценки рисков информационной безопасности, проводимых подразделением (ответственным работником) по информационной безопасности;

8) разработка и формирование реестра рисков, включающего риски информационной безопасности;

9) предоставление отчетности о реализации существенных рисков информационной безопасности и мониторинг исполнения мероприятий по устранению их последствий органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

10) предоставление отчетности или иной информации по управлению рисками информационной безопасности органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

11) использование результатов внутреннего аудита в части рисков информационной безопасности.

51. ПУЦА создает структурное подразделение (назначает ответственного работника) по информационной безопасности, в функции которого входит:

1) проведение оценки рисков информационной безопасности;

2) разработка мер по обработке рисков информационной безопасности и предоставление отчетности по их реализации в подразделение (ответственному работнику) по управлению рисками;

3) подготовка и предоставление отчетности о реализации существенных рисков информационной безопасности в подразделение рисков ПУЦА, а также об устранении их последствий;

4) разработка планов мероприятий по реализации стратегии ПУЦА в части обеспечения информационной безопасности.

ПУЦА обеспечивает раздельное функционирование структурного подразделения (ответственного работника) по управлению рисками от структурного подразделения (ответственного работника) по информационной безопасности.

52. Подразделение (ответственный работник) по управлению рисками разрабатывает внутренний документ, определяющий порядок управления рисками информационной безопасности, который включает, но не ограничивается:

1) процедуры идентификации и классификации информационных активов, с целью выявления критичных информационных активов;

2) процедуры идентификации уязвимостей критичных информационных активов;

3) процедуры идентификации потенциальных угроз в отношении критичных информационных активов;

4) процедуры идентификации существующих мер управления рисками информационной безопасности;

5) процедуры оценки вероятности и последствий нарушения конфиденциальности, целостности и доступности информационных активов, применяя качественные и (или) количественные методы оценки, в том числе на основании данных об их реализации;

6) процедуры сбора и хранения сведений о реализации существенных рисков информационной безопасности;

7) процедуры формирования реестра рисков, включающего риски информационной безопасности;

8) процедуры мониторинга исполнения мер по обработке рисков информационной безопасности.".

Председатель Национального Банка Республики Казахстан *Т. Сулейменов*

Утверждены
постановлением
Председатель
Национального Банка
Республики Казахстан
от 29 апреля 2026 года № 47

Правила формирования системы управления рисками и внутреннего контроля для операторов обмена необеспеченных цифровых активов, операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов

Глава 1. Общие положения

1. Настоящие Правила формирования системы управления рисками и внутреннего контроля для операторов обмена необеспеченных цифровых активов, операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов (далее – Правила) разработаны в соответствии с подпунктом 10) части второй пункта 1 статьи 4 Закона Республики Казахстан "О цифровых активах в Республике Казахстан" (далее – Закон о цифровых активах) и определяют порядок формирования системы управления рисками и внутреннего контроля для операторов обмена необеспеченных цифровых активов, операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов (далее – ПУЦА).

2. В Правилах используются понятия, предусмотренные Законом о цифровых активах и Законом Республики Казахстан "О рынке ценных бумаг", а также следующие понятия:

1) информационный актив – совокупность информации и объекта цифровой инфраструктуры, используемого для ее хранения и (или) обработки;

2) риски мошенничества и противоправных инцидентов – вероятность возникновения финансовых потерь и репутационных рисков, вовлечения ПУЦА в противоправные действия вследствие мошенничества со стороны третьих лиц и (или) работников ПУЦА, использования услуг с цифровыми активами в операциях, связанных с незаконным производством, оборотом и (или) транзитом наркотиков, организацией деятельности финансовых пирамид и для осуществления платежей и (или) переводов денег в пользу электронного казино и интернет-казино, а также иностранных букмекерских контор и (или) тотализаторов, не имеющих лицензий на право занятия деятельностью в сфере игорного бизнеса в Республике Казахстан;

3) ценовой риск – вероятность возникновения расходов (убытков) вследствие изменения стоимости цифровых активов и финансовых инструментов, возникающий в случае изменения условий рынка цифровых активов и финансовых рынков, влияющих на рыночную стоимость цифровых активов и финансовых инструментов, приобретенных за счет собственных активов ПУЦА;

4) репутационный риск – вероятность возникновения расходов (убытков) вследствие негативного общественного мнения или снижения доверия к ПУЦА;

5) бэк-тестинг – методы проверки эффективности процедур измерения рисков с использованием исторических данных по ПУЦА и сравнением рассчитанных результатов с текущими (фактическими) результатами от совершения указанных операций;

6) валютный риск – вероятность возникновения расходов (убытков), связанных с изменением курсов иностранных валют при осуществлении ПУЦА своей деятельности. Опасность расходов (убытков) возникает из-за переоценки позиций по валютам в стоимостном выражении;

7) юридический (правовой) риск – риск возникновения расходов (убытков) вследствие нарушения ПУЦА требований законодательства Республики Казахстан, в том числе несоответствия внутренних документов ПУЦА требованиям нормативных правовых актов Национального Банка Республики Казахстан, несоответствия практики деятельности ПУЦА его внутренним документам, а в отношениях с нерезидентами Республики Казахстан – нарушения требований законодательства других государств, а также условий заключенных договоров;

8) риск кибербезопасности – вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов ПУЦА;

9) кредитный риск – вероятность возникновения расходов (убытков) вследствие неисполнения эмитентом цифровых финансовых активов или контрагентом своих обязательств по выпущенным цифровым финансовым активам или заключенным сделкам в соответствии с оговоренными условиями, а также неуплаты или несвоевременной оплаты клиентами услуг ПУЦА;

10) корпоративное управление – система стратегического и тактического управления ПУЦА, представляющая собой комплекс взаимоотношений между высшим органом, органом управления, исполнительным органом и иными органами ПУЦА, направленная на обеспечение эффективного функционирования ПУЦА, защиту прав и интересов его акционеров (участников), и предоставляющая акционерам (участникам) возможность эффективного контроля и мониторинга деятельности ПУЦА;

11) комплаенс-риск – вероятность возникновения потерь вследствие несоблюдения ПУЦА и его работниками требований гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее – ПОД/ФТ/ФРОМУ), об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью, внутренних документов ПУЦА, регламентирующих порядок оказания услуг и проведения операций на рынке цифровых активов, а также законодательства иностранных государств, оказывающего влияние на деятельность ПУЦА;

12) критичный вид деятельности – вид деятельности, от бесперебойности осуществления которой зависит устойчивость ПУЦА в целом;

13) политика инвестирования собственных активов – документ, определяющий перечень объектов инвестирования, цели, стратегии, условия и ограничения инвестиционной деятельности в отношении собственных активов ПУЦА, условия хеджирования и диверсификации собственных активов ПУЦА;

14) конфликт интересов – ситуация, при которой возникает противоречие между личной заинтересованностью должностных лиц ПУЦА, его акционеров (участников) и (или) его работников и надлежащим исполнением ими своих должностных полномочий или имущественными и иными интересами ПУЦА и (или) его работников и (или) клиентов, которое повлечет за собой неблагоприятные последствия для ПУЦА и (или) его клиентов. ПУЦА, действуя в качества ПУЦА, исходит из приоритета интересов клиента над своими интересами, интересами своих работников, акционеров (участников) и аффилированных лиц;

15) операционный риск – вероятность возникновения расходов (убытков) в результате недостатков или ошибок в ходе осуществления внутренних процессов, допущенных со стороны работников (человеческих ресурсов) и ходе ненадлежащего

функционирования цифровых систем, цифровых платформ (торговых платформ) и технологий, а также вследствие влияния внешних событий, за исключением стратегического риска и репутационного риска;

16) риск потери ликвидности – риск, связанный с возможным невыполнением либо несвоевременным выполнением ПУЦА своих обязательств. Риск потери ликвидности цифровых активов определяется возможностью их быстрой реализации с низкими издержками и по приемлемым ценам;

17) стратегический риск – вероятность возникновения убытков в результате ошибок (недостатков), допущенных при принятии решений, определяющих стратегическое развитие ПУЦА и выражающихся в недостаточном учете возможных опасностей, присущих деятельности ПУЦА, неправильном или недостаточно обоснованном определении перспективных направлений деятельности, в которых ПУЦА достигнет преимущества перед конкурентами, отсутствии или обеспечении в неполном объеме необходимых ресурсов и организационных мер, обеспечивающих достижение стратегических целей деятельности ПУЦА;

18) стресс-тестирование – методы измерения потенциального влияния на финансовое положение ПУЦА исключительных, но возможных событий, которые оказывают влияние на деятельность ПУЦА;

19) стрессовые ситуации – непредвиденные ситуации возникновения перегрузок, сбоев, ошибок и (или) иных неполадок в работе систем (цифровых платформ, торговых платформ) ПУЦА;

20) риск – вероятность того, что ожидаемые или непредвиденные события окажут отрицательное влияние на деятельность ПУЦА, его капитал и (или) доходы;

21) риск-профиль – совокупность видов риска и иных сведений, характеризующих степень подверженности ПУЦА рискам, присущим всем видам деятельности ПУЦА для выявления слабых сторон и определения приоритетности последующих действий в рамках системы управления рисками;

22) риск-аппетит – агрегированный (агрегированные) уровень (уровни) существенных рисков (лимиты допустимого размера риска), который (которые) ПУЦА готов принять либо намерен исключить при реализации стратегии;

23) система управления рисками – совокупность взаимосвязанных элементов: процедур, методик, цифровых систем, объединенных в единый процесс по управлению реализованными и потенциальными рисками в рамках приемлемого для акционера (участника) уровня риска и направленных на достижение целей и задач по управлению рисками. В процессе выявления и управления реализованными и потенциальными рисками, влияющими на деятельность ПУЦА, участвуют органы ПУЦА, руководящие работники и работники структурных подразделений (ответственные работники) в

пределах закрепленной компетенции и ответственности. Процесс выявления и управления реализованными и потенциальными рисками включает в себя оценку риска , измерение риска, контроль риска и мониторинг риска;

24) матрица рисков – инструментарий для выявления, оценки и визуализации потенциальных рисков в порядке, предусмотренном внутренним документом ПУЦА;

25) риск-культура – процессы, процедуры, внутренние правила ПУЦА, направленные на понимание, принятие, управление и контроль за рисками с целью минимизации их влияния на деятельность ПУЦА, а также этические нормы и стандарты профессиональной деятельности всех участников организационной структуры;

26) организационная структура – количественный состав и система органов управления (исполнительных органов), руководящих работников и структурных подразделений ПУЦА, отражающие структуру подчиненности, подотчетности, предусмотренные внутренним документом и (или) совокупностью внутренних документов ПУЦА;

27) риск цифровых технологий – вероятность возникновения ущерба вследствие отказа (нарушения функционирования) цифровых технологий, эксплуатируемых ПУЦА;

28) служба внутреннего аудита (ответственный работник по внутреннему аудиту) – подразделение (ответственный работник) ПУЦА, созданное в соответствии с законодательством Республики Казахстан об (о) акционерных обществах и товариществах с ограниченной и дополнительной ответственностью в зависимости от организационно-правовой формы ПУЦА;

29) система внутреннего контроля – часть системы управления рисками, представляющая совокупность процедур и политик внутреннего контроля, обеспечивающих реализацию ПУЦА долгосрочных целей рентабельности и поддержания надежной системы финансовой и управленческой отчетности, способствующей соблюдению законодательства Республики Казахстан, политики ПУЦА, внутренних правил и процедур, снижению риска убытков или репутационного риска ПУЦА;

30) внутренние документы – документы, регулирующие условия и порядок деятельности ПУЦА, его органов, подразделений (ответственных работников) и работников подразделений.

Глава 2. Организация системы управления рисками

3. Целью Правил является определение требований к формированию ПУЦА систем управления рисками и внутреннего контроля путем обеспечения:

1) эффективного управления рисками ПУЦА посредством своевременного их выявления, измерения, контроля и мониторинга для обеспечения соответствия

деятельности ПУЦА, выбранной бизнес модели, требованиям по корпоративному управлению, функционированию цифровых систем, цифровых платформ (торговых платформ) и систем управленческой информации, проведению разрешенных операций, управлению активами и обязательствами, функционированию системы учета ПУЦА и иных цифровых и коммуникационных систем ПУЦА, а также уровню принимаемых им рисков и наличия соответствующего уровня ликвидности;

2) надлежащей практики корпоративного управления и надлежащего уровня деловой этики и риск-культуры;

3) соблюдения ПУЦА и его работниками требований гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о ПОД/ФТ/ФРОМУ, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью, внутренних политик, процедур и иных внутренних документов ПУЦА, регламентирующих порядок оказания услуг и проведения операций на рынке цифровых активов, а также законодательства иностранных государств, оказывающего влияние на деятельность ПУЦА;

4) своевременного обнаружения и устранения недостатков в деятельности ПУЦА и его работников;

5) создания в ПУЦА адекватных механизмов для решения непредвиденных или чрезвычайных ситуаций;

6) рационального принятия решений и действий в интересах ПУЦА на основании всесторонней оценки предоставляемой информации добросовестно, с должной осмотрительностью и заботливостью (duty of care);

7) принятия решений работниками и должностными лицами ПУЦА добросовестно;

8) распределения функций, обязанностей и полномочий управления рисками между всеми структурными подразделениями и работниками ПУЦА, и их ответственности с учетом минимизации конфликта интересов;

9) разделения функции управления рисками и внутреннего контроля от операционной деятельности ПУЦА посредством построения системы трех линий защиты, которая включает:

первую линию – на уровне структурных подразделений или сотрудников бизнес подразделений ПУЦА;

вторую линию – на уровне подразделения (ответственного работника) по управлению рисками и выполняющих контрольные функции;

третью линию – на уровне подразделения (ответственного работника) внутреннего аудита в части оценки эффективности функционирования системы управления рисками ;

ПУЦА применяет риск-ориентированный подход в формировании трех линий защиты, который предполагает учет своего размера, значимости, характера, масштаба и сложности деятельности ПУЦА.

Информационный обмен между подразделениями (ответственными работниками) ПУЦА по вопросам управления рисками и внутреннего контроля осуществляется в соответствии с внутренними документами.

10) наличия документов, разработанных в целях регламентирования деятельности ПУЦА, создания и функционирования у ПУЦА эффективных систем управления рисками и внутреннего контроля и соответствующих стратегии, организационной структуре, профилю рисков ПУЦА и требованиям гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о ПОД/ФТ/ФРОМУ, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью, а также их периодического пересмотра и актуализации;

11) соблюдения действующих процедур, процессов, политик и иных внутренних документов ПУЦА по управлению рисками посредством построения эффективной системы внутреннего контроля.

4. ПУЦА не реже одного раза в год в порядке, предусмотренном внутренним документом ПУЦА, проводит стресс-тестирование по основным рискам, которым подвержена деятельность ПУЦА.

Стресс-тестирование по операционному риску в части организации и проведения торгов проводится путем тестирования торговой платформы оператора торговой платформы цифровых активов на:

1) моделирование стрессовых ситуаций функционирования элементов торговой платформы, включающих в себя количество пользовательских подключений, пропускную способность потоков информации, скорость подачи заявок и заключения сделок, отказ компонентов торговой платформы на основных и (или) вспомогательных серверах;

2) на подборку, комбинирование и моделирование стрессовых ситуаций и параметров функционирования элементов торговой платформы, включая сетевые соединения, операционную систему, базу данных, уровень авторизации (доступа) к торговой платформе, количество пользователей, потоки информации, объемы торгов,

нагрузку на основной и (или) вспомогательный сервер (с указанием уровня критической нагрузки).

5. ПУЦА не реже одного раза в год в порядке, предусмотренном внутренним документом ПУЦА, проводит бэк-тестинг, а именно проверки эффективности процедур измерения рисков с использованием исторических данных по деятельности ПУЦА и сравнением рассчитанных в результате проведения стресс-тестирования результатов с текущими (фактическими) результатами от совершения операций с цифровыми активами и (или) финансовыми инструментами.

6. ПУЦА представляет результаты стресс-тестирований и бэк-тестингов с предложениями по совершенствованию процедур управления рисками (при необходимости) органу управления (исполнительному органу, наблюдательному совету – при наличии), который использует результаты оценки рисков и регулярных стресс-тестирований и бэк-тестингов при принятии решений в отношении деятельности ПУЦА и совершения сделок с цифровыми активами и (или) финансовыми инструментами.

7. Система управления рисками ПУЦА включает следующие направления его деятельности:

1) проведение и администрирование процесса расчетов и (или) торгов по операциям с цифровыми активами и деньгами;

2) сбор, ввод, хранение и распространение информации, представляемой эмитентами цифровых финансовых активов и клиентами ПУЦА (эмитент цифровых финансовых активов не предоставляет информацию оператору обмена необеспеченных цифровых активов);

3) проведение регулярного мониторинга систем учета, иных цифровых и коммуникационных систем (цифровых платформ, торговых платформ) в целях обеспечения бесперебойности, непрерывности деятельности процесса оказания услуг цифровых активов для ПУЦА (за исключением оператора обмена необеспеченных цифровых активов), учета прав по цифровым активам и иным финансовым инструментам, расчетов в цифровых активах и (или) деньгах, а также отражения сведений, содержащихся в соответствующих системах учета;

4) проведение ежегодного внутреннего аудита программно-технического обеспечения ПУЦА, включая цифровые и коммуникационные системы, используемые ПУЦА в своей деятельности;

5) разработка и реализация проектов, направленных на дальнейшее развитие и совершенствование деятельности ПУЦА в части функционирования систем учета, цифровых и коммуникационных систем (цифровых платформ, торговых платформ), процесса оказания услуг цифровых активов для ПУЦА, учета ПУЦА (за исключением оператора обмена необеспеченных цифровых активов) прав по цифровым активам, расчетов в цифровых активах, отражения сведений, содержащихся в системах учета,

автоматизации отдельных операций, совершаемых в ПУЦА, а также процесса сбора, ввода, учета, хранения информации и иных направлений деятельности ПУЦА;

6) разработка и утверждение внутренних документов, в том числе политики инвестирования собственных активов ПУЦА в цифровые активы и (или) финансовые инструменты в соответствии с порядком, предусмотренном внутренним документом ПУЦА;

7) создание и совершенствование организационно-функциональной структуры управления ПУЦА;

8) представление информации, необходимой для принятия решений, заинтересованным органам ПУЦА и обмен информацией между органами и подразделениями (ответственными работниками) ПУЦА;

9) мониторинг соблюдения ПУЦА и его работниками требований, установленных законодательством Республики Казахстан о цифровых активах, о рынке ценных бумаг, внутренней политикой ПУЦА в области управления рисками;

10) определение порядка организации ПУЦА работы с клиентами, в том числе определение процедур по рассмотрению и разрешению споров, а также порядка применения операторами платформы цифровых финансовых активов и (или) операторами торговой платформы цифровых активов соответствующих мер в случае невыполнения клиентами, в том числе эмитентами цифровых финансовых активов и держателями цифровых финансовых активов, своих обязательств;

11) формирование, ведение и хранение ПУЦА информации об операциях (сделках) в системе учета ПУЦА.

Положения настоящих Правил применяется к фондовой бирже в части, не урегулированной постановлением Правления Национального Банка Республики Казахстан от 19 декабря 2015 года № 252 "Об утверждении Правил формирования системы управления рисками и внутреннего контроля для фондовой биржи" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 12999).

Положения настоящих Правил применяется к центральному депозитарию в части, не урегулированной постановлением Постановление Правления Национального Банка Республики Казахстан от 28 декабря 2018 года № 318 "Об утверждении Правил формирования системы управления рисками и внутреннего контроля для центрального депозитария" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 18180).

8. Система управления рисками предусматривает, но не ограничивается, наличием следующих внутренних документов:

1) политика ПУЦА по управлению рисками;

2) порядок (политика) инвестирования собственных активов ПУЦА;

3) процедуры осуществления внутреннего контроля и внутреннего аудита;

4) процедуры, направленные на ПОД/ФТ/ФРОМУ;

5) процедуры управления ПУЦА существующими и потенциальными конфликтами интересов;

6) процедуры, направленные на предотвращение использования инсайдерской информации руководящими и иными работниками ПУЦА;

7) порядок осуществления расчетов по заключенным сделкам с цифровыми активами;

8) процедуры перевода цифровых активов и порядок сбора и хранения информации об отправителе и получателе цифровых активов;

9) информационная политика ПУЦА;

10) инструкция по технике безопасности.

11) политики управления рисками мошенничества и противоправных инцидентов.

Риск-культура дополняет существующие утвержденные процедуры, процессы и механизмы деятельности ПУЦА и является неотъемлемым компонентом системы управления рисками.

9. ПУЦА на ежегодной основе осуществляет оценку системы управления рисками и внутреннего контроля (далее – Ежегодная оценка) по форме согласно приложению к Правилам и в порядке, предусмотренном внутренними документами ПУЦА.

10. По итогам Ежегодной оценки оформляется отчет об оценке выполнения требований к системе управления рисками по форме согласно приложению к Правилам , который направляется в Национальный Банк Республики Казахстан не позднее первого квартала, следующего за отчетным годом.

11. Задачами формирования системы управления рисками являются:

1) своевременное выявление рисков и угроз;

2) повышение качества оценки максимально допустимых значений показателей рисков;

3) развитие альтернативных механизмов контроля рисков;

4) обеспечение принятия своевременных мер по минимизации и управлению рисками;

5) вовлечение отдельных структурных подразделений ПУЦА (отдельных линий защиты), включая подразделение по управлению рисками, в процесс мониторинга и оценки рисков, а также повышение ответственности работников ПУЦА в области системы управления рисками.

12. Система управления рисками ПУЦА включает идентификацию, измерение, оценку, контроль и мониторинг риска, которые осуществляются в соответствии с порядком, предусмотренным внутренними документами ПУЦА.

13. Руководитель подразделения ПУЦА по управлению рисками (ответственные работники по управлению рисками) и (или) работники подразделения ПУЦА по управлению рисками имеют высшее образование, обладают профессиональной

компетентностью и опытом работы не менее трех лет в области управления рисками, а также обладают знаниями финансового законодательства Республики Казахстан и законодательства Республики Казахстан о цифровых активах, рынке ценных бумаг.

14. Дополнительные требования к руководителю и работникам подразделения по управлению рисками устанавливаются ПУЦА.

15. ПУЦА в своей деятельности идентифицирует и дифференцирует следующие типы (виды) рисков:

1) операционные риски;

2) юридические (правовые) риски;

3) репутационные риски;

4) рыночные (ценовые, валютные и процентные) риски;

5) кредитные риски;

6) риски потери ликвидности;

7) риски, определяемые в соответствии с политикой ПУЦА по управлению рисками

.

16. Целями процесса идентификации, оценки и контроля рисков являются:

1) своевременное определение неидентифицированных рисков и угроз;

2) повышение качества оценки максимально допустимых значений показателей рисков;

3) развитие альтернативных механизмов контроля рисков;

4) обеспечение принятия своевременных мер по минимизации и управлению рисками;

5) вовлечение отдельных подразделений ПУЦА (ответственных работников), включая подразделение по управлению рисками (ответственного работника по управлению рисками), в процесс идентификации и оценки рисков, а также увеличение ответственности работников ПУЦА в области управления рисками.

17. Процедура идентификации рисков основывается на тщательном обзоре и мониторинге, осуществляемых каждым подразделением ПУЦА в зависимости от вида деятельности подразделения совместно с подразделением по управлению рисками (ответственным работником по управлению рисками).

Идентифицированные риски анализируются по следующим характеристикам:

1) частота наступления рисков;

2) масштаб воздействия рисков.

На основе результатов анализа риски дифференцируются как приемлемые и неприемлемые в зависимости от значения показателя рисков, определенного в качестве допустимого.

18. Подразделение правового обеспечения (юридическое подразделение или ответственный работник по правовому обеспечению) ПУЦА обеспечивает регулирование юридических (правовых) рисков, возникающих вследствие нарушения

ПУЦА требований законодательства Республики Казахстан, в том числе несоответствия внутренних документов ПУЦА требованиям нормативных правовых актов Национального Банка Республики Казахстан, несоответствия практики деятельности ПУЦА ее внутренним документам, а также условий заключенных договоров.

19. Подразделение (ответственный работник) ПУЦА по отношениям с общественностью совместно с подразделением по управлению рисками обеспечивает контроль, мониторинг, а также минимизацию репутационных рисков в порядке, предусмотренном внутренними документами ПУЦА.

20. ПУЦА ежегодно не позднее 1 апреля года, следующего за отчетным, представляет в Национальный Банк Республики Казахстан отчет об оценке выполнения требований к системе управления рисками по форме согласно приложению к Правилам .

Глава 3. Бизнес модель

21. Бизнес модель ПУЦА – это совокупность выбранной стратегии, продуктов, процессов планирования, обеспечивающих конкурентоспособность и достаточный уровень доходности ПУЦА.

22. Основными принципами при формировании бизнес модели ПУЦА являются:

1) жизнеспособность, выражающаяся в способности ПУЦА обеспечивать достаточный уровень доходности в ближайшие 12 (двенадцать) месяцев и основанная на бюджетном планировании и прогнозировании финансовых показателей;

2) устойчивость, выражающаяся в способности ПУЦА обеспечивать достаточный уровень доходности на период не менее 3 (трех) лет и основанная на стратегическом планировании и прогнозировании финансовых показателей.

ПУЦА проводит регулярный анализ бизнес модели в целях оценки влияния на нее стратегических рисков и рисков, присущих деятельности ПУЦА.

Деятельность ПУЦА осуществляется в рамках выбранной бизнес модели с учетом объема активов, характера и уровня сложности деятельности, организационной структуры, риск-профиля.

23. Стратегия ПУЦА утверждается органом управления (исполнительным органом, наблюдательным советом – при наличии) ПУЦА на период не менее 3 (трех) лет.

24. Содержание (структура) стратегии ПУЦА определяется внутренними документами ПУЦА.

25. Стратегия ПУЦА составляется и совершенствуется с учетом результатов бэк-тестинга для исключения факторов, ранее негативно отразившихся на деятельности ПУЦА.

Глава 4. Стратегия риск-аппетита

26. В целях построения эффективной системы управления рисками орган управления (исполнительный орган, наблюдательный совет – при наличии) ПУЦА утверждает стратегию риск-аппетита в качестве отдельного документа, либо как составной части стратегии ПУЦА.

27.Стратегия риск-аппетита определяет четкие границы объема принимаемых рисков, в которых осуществляется деятельность ПУЦА в рамках реализации общей стратегии ПУЦА, а также определяет риск-профиль деятельности ПУЦА с целью недопущения реализации рисков либо минимизации их отрицательного влияния на деятельность ПУЦА. Стратегия риск-аппетита учитывается:

1) при стратегическом и бюджетном планировании ПУЦА, определенных главой 3 Правил;

2) при формировании организационной структуры ПУЦА и политики оплаты труда, определенных главой 5 Правил.

28. ПУЦА при разработке стратегии риск-аппетита учитывает размер своих активов , долю на рынке, характер, масштаб и сложность своей деятельности.

Глава 5. Корпоративное управление

29. Основными элементами эффективной системы корпоративного управления являются:

1) организационная структура;

2) корпоративные ценности;

3) стратегия деятельности ПУЦА;

4) распределение обязанностей и полномочий в части принятия решений между органами ПУЦА;

5) механизмы взаимодействия и сотрудничества между органами ПУЦА, внешними и внутренними аудиторами ПУЦА;

6) процедуры и методики управления рисками;

7) система внутреннего контроля;

8) система вознаграждения;

9) наличие системы управленческой отчетности;

10) прозрачность корпоративного управления.

30. Организационная структура ПУЦА соответствует выбранной бизнес-модели, профилю рисков, масштабу и характеру деятельности, видам и сложности операций, минимизирует конфликт интересов и распределяет полномочия по управлению рисками между коллегиальными органами и структурными подразделениями (ответственными работниками), и соответствует требованиям, установленным законами

Республики Казахстан об (о) акционерных обществах, товариществах с ограниченной и дополнительной ответственностью (в зависимости от организационно-правовой формы ПУЦА).

Организационная структура определяется ПУЦА с учетом размера своих активов, доли на рынке, характера, масштаба и сложности деятельности ПУЦА.

Глава 6. Управление непрерывностью деятельности

31. ПУЦА осуществляет в порядке, определенном внутренним документом ПУЦА, анализ влияния на деятельность, посредством которого осуществляется оценка:

1) воздействий, повреждений или потерь на персонал, помещения, технологии или информацию ПУЦА;

2) нарушений требований гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о ПОД/ФТ/ФРОМУ, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью;

3) потери репутации.

32. ПУЦА идентифицирует критичные виды деятельности. Идентифицированная в процессе анализа влияния на деятельность ПУЦА, потеря которой оказывает в краткосрочный период времени максимальное негативное воздействие на ПУЦА и подлежит восстановлению в кратчайшие сроки, является критичным видом деятельности.

33. ПУЦА определяет ресурсы и меры управления рисками непредвиденных обстоятельств, необходимые для поддержания критичных видов деятельности, которые включают, но не ограничиваются следующим:

1) персонал (необходимое количество работников, необходимые навыки и компетенции);

2) помещения (основные и альтернативные площадки, а также помещения, требующие повышенной защиты);

3) технологии (информационно-технологические и телекоммуникационные услуги, поддерживающие критичные виды деятельности, а также прочие технологии, поддерживающие критичные виды деятельности, в том числе охрана периметра);

4) информация (необходимая информация для выполнения критичных видов деятельности, объем информации, требующей восстановления, а также методы и способы хранения, защиты и восстановления информации);

5) поставщики, внешние услуги и снабжение, от которых зависит выполнение критичных видов деятельности;

6) финансовые ресурсы (объем финансовых ресурсов, потенциально доступный для исполнения плана обеспечения непрерывности и восстановления деятельности ПУЦА в случае возникновения непредвиденных обстоятельств).

34. ПУЦА осуществляет анализ рисков непредвиденных обстоятельств, который позволяет оценить угрозы и уязвимость в критичных видах деятельности и используемых ими ресурсах. В качестве угроз, которые оказывают негативное воздействие на ресурсы, ПУЦА рассматривает, но, не ограничиваясь, следующее:

1) недоступность работников;

2) недоступность технологий, в том числе цифровых и коммуникационных технологий (компьютерные вирусы, отказ компьютерных аппаратных средств, потеря связи);

3) недоступность снабжения (воды, электричества);

4) отсутствие доступа к зданиям (помещениям);

5) недоступность ключевых поставщиков, контрагентов;

6) недоступность ключевой информации;

7) недоступность финансовых ресурсов.

35. ПУЦА обеспечивает разработку и наличие плана (планов) по обеспечению непрерывности и (или) восстановлению деятельности. План (планы) по обеспечению непрерывности и (или) восстановлению деятельности должен учитывать размер своих активов, долю на рынке, характер, масштаб и сложность своей деятельности.

Глава 7. Управление рыночным риском

36. Исполнительный орган и (или) глава риск-менеджмента (ответственный работник по управлению рисками) ПУЦА обеспечивает разработку политики управления рыночным риском и осуществляет мониторинг и контроль за соблюдением ПУЦА и его работниками политики управления рыночным риском, которая соответствует масштабу деятельности ПУЦА, текущей рыночной ситуации, стратегии, размеру и уровню сложности операций ПУЦА и обеспечивает эффективное выявление, измерение, мониторинг и контроль за рыночным риском ПУЦА.

37. Способы (меры) по снижению рыночных рисков ПУЦА (лимиты, нормы диверсификации, хеджирование, резервирование, страхование и иные способы) определяются внутренними документами ПУЦА.

Глава 8. Управление риском потери ликвидности

38. ПУЦА разрабатывает эффективный процесс по выявлению, оценке, мониторингу и контролю риска потери ликвидности, который включает детальное прогнозирование денежных потоков по активам, обязательствам и внебалансовым инструментам на разных временных интервалах.

39. ПУЦА оценивает все балансовые и внебалансовые статьи, влияющие на уровень риска потери ликвидности. ПУЦА оценивает уровень ликвидности на рынке для покрытия потребности ПУЦА в привлечении фондирования в целях регулирования риска потери ликвидности.

40. При управлении риском потери ликвидности ПУЦА учитывает снижение стоимости активов и влияния их продажи во время стрессов на уровень ликвидности, доходности и капитал.

41. ПУЦА учитывает взаимодействие между риском потери ликвидности и другими видами рисков, которым он подвергается.

Глава 9. Управление операционным риском

42. К операционным рискам относятся риски, связанные с:

1) неопределенной и неэффективной организационной структурой ПУЦА, включая распределение ответственности, структуру подотчетности и управления;

2) неэффективными стратегиями, политиками и (или) стандартами в области цифровых технологий, недостатками в использовании программного обеспечения;

3) неэффективным управлением персоналом и (или) неквалифицированным штатом ПУЦА;

4) несанкционированным использованием систем учета, цифровых платформ (торговых платформ);

5) рисками, связанными с недостаточно эффективным построением процессов осуществления деятельности ПУЦА либо слабым контролем соблюдения внутренних правил;

6) непредвиденными или неконтролируемыми факторами внешнего воздействия на деятельность ПУЦА;

7) наличием недостатков или ошибок во внутренних документах, регламентирующих деятельность ПУЦА;

8) нарушением процесса регистрации сделок, расчетов с цифровыми активами, отражения сведений, содержащихся в системах учета отдельных операций, совершаемых в ПУЦА, и совершения операций в указанных системах;

9) неправомерным использованием конфиденциальной информации, предоставляемой клиентами ПУЦА;

10) возникновением конфликта интересов между органами ПУЦА и его подразделениями;

11) возникновением ошибок, связанных со сбором, вводом, хранением и распространением информации;

12) вероятностью возникновения ошибок и сбоев в функционировании программно-технического обеспечения ПУЦА, включая соответствующие системы

учета, а также в эксплуатируемых цифровых и коммуникационных системах и технологиях;

13) вероятностью возникновения ущерба вследствие использования несовершенных технологий в процессе деятельности ПУЦА, включая, в том числе процессы организации учета прав по цифровым активам, регистрации сделок, расчетов сделок с цифровыми активами, отражения сведений, содержащихся в системах учета (по учету в отношении операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов), исполнения функций системного администрирования;

14) возникновением ошибок при вводе и изменении данных в системах учета (по учету в отношении операторов платформы цифровых финансовых активов, операторов торговой платформы цифровых активов);

15) обстоятельствами, идентифицируемыми ПУЦА в качестве потенциальных рисков.

43. При измерении, оценке, контроле и мониторинге операционных рисков ПУЦА применяет один или несколько из следующих методов:

1) применение ключевых индикаторов риска;

2) формирование матрицы рисков;

3) осуществление сбора и анализ внутренних данных по убыткам (ведение базы данных по убыткам);

4) описание (регламентация) бизнес-процессов;

5) использование результатов внутреннего аудита.

Порядок выбора методов измерения, оценки, контроля, мониторинга и способов (мер) по снижению операционных рисков устанавливается внутренним документом ПУЦА по вопросам управления операционными рисками.

Глава 10. Управление рисками цифровых технологий

44. Система управления рисками цифровых технологий включает, но не ограничивается:

1) политику управления рисками цифровых технологий;

2) процедуры управления рисками цифровых технологий;

3) систему управленческой информации;

4) оценку эффективности системы управления рисками цифровых технологий подразделением внутреннего аудита (ответственным работником по внутреннему аудиту).

45. ПУЦА определяет следующих участников системы управления рисками цифровых технологий (но не ограничиваясь ими):

1) подразделение (ответственный работник) по управлению рисками ПУЦА;

2) подразделение (ответственный работник) по цифровым технологиям.

46. ПУЦА создает структурное подразделение (назначает ответственного работника) по управлению рисками, в функции которого входит управление рисками цифровых технологий, включая:

1) разработку, внедрение и развитие системы управления рисками цифровых технологий;

2) участие в разработке и согласовании планов мероприятий по реализации стратегии ПУЦА в части обеспечения доступности цифровых технологий;

3) участие в оценке рисков цифровых технологий;

4) мониторинг уровня рисков цифровых технологий;

5) взаимодействие и консультирование структурных подразделений (ответственного работника) ПУЦА по вопросам управления рисками цифровых технологий;

6) планирование проведения и анализ результатов оценки рисков цифровых технологий, проводимой подразделением (ответственным работником) по цифровым технологиям;

7) разработка и формирование реестра рисков, включающего риски цифровых технологий;

8) предоставление отчетности о реализации существенных рисков цифровых технологий и мониторинг исполнения мероприятий по устранению их последствий органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

9) предоставление отчетности или иной информации по управлению рисками цифровых технологий органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

10) использование результатов внутреннего аудита в части рисков цифровых технологий.

47. ПУЦА создает структурное подразделение (назначает ответственного работника) по цифровым технологиям, в функции которого входит:

1) проведение оценки рисков цифровых технологий;

2) разработка мер по обработке рисков цифровых технологий и предоставление отчетности по их реализации в подразделение по управлению рисками;

3) подготовка и предоставление отчетности о реализации существенных рисков цифровых технологий в подразделение рисков ПУЦА, а также об устранении их последствий;

4) разработка планов мероприятий по реализации стратегии ПУЦА в части обеспечения доступности цифровых технологий для критичных бизнес-процессов.

Глава 11. Управление рисками кибербезопасности

48. Система управления рисками кибербезопасности включает, но не ограничивается:

1) политику управления рисками кибербезопасности;

2) процедуры управления рисками кибербезопасности;

3) систему управленческой информации;

4) оценку эффективности системы управления рисками кибербезопасности подразделением внутреннего аудита (ответственным работником по внутреннему аудиту).

49. ПУЦА определяет следующих участников системы управления рисками кибербезопасности (но не ограничиваясь ими):

1) подразделение (ответственный работник) по управлению рисками ПУЦА;

2) подразделение (ответственный работник) по кибербезопасности;

3) подразделение (ответственный работник) по цифровым технологиям;

4) подразделения-владельцы защищаемой информации.

50. ПУЦА создает структурное подразделение (назначает ответственного работника) по управлению рисками, в функции которого входит управление рисками кибербезопасности:

1) разработка, внедрение и развитие системы управления рисками кибербезопасности;

2) участие в разработке и согласовании планов мероприятий по реализации стратегии ПУЦА в части обеспечения кибербезопасности;

3) создание и руководство рабочей группой по формированию перечня критичных информационных активов ПУЦА, включающей как минимум подразделения-владельцев защищаемой информации;

4) участие в оценке рисков кибербезопасности;

5) мониторинг уровня рисков кибербезопасности;

6) взаимодействие и консультирование структурных подразделения ПУЦА (ответственного работника) по вопросам управления рисками кибербезопасности;

7) планирование проведения и анализ результатов оценки рисков кибербезопасности, проводимых подразделением (ответственным работником) по кибербезопасности;

8) разработка и формирование реестра рисков, включающего риски кибербезопасности;

9) предоставление отчетности о реализации существенных рисков кибербезопасности и мониторинг исполнения мероприятий по устранению их последствий органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

10) предоставление отчетности или иной информации по управлению рисками кибербезопасности органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

11) использование результатов внутреннего аудита в части рисков кибербезопасности.

51. ПУЦА создает структурное подразделение (назначает ответственного работника) по кибербезопасности, в функции которого входит:

1) проведение оценки рисков кибербезопасности;

2) разработка мер по обработке рисков кибербезопасности и предоставление отчетности по их реализации в подразделение (ответственному работнику) по управлению рисками;

3) подготовка и предоставление отчетности о реализации существенных рисков кибербезопасности в подразделение рисков ПУЦА, а также об устранении их последствий;

4) разработка планов мероприятий по реализации стратегии ПУЦА в части обеспечения кибербезопасности.

ПУЦА обеспечивает раздельное функционирование структурного подразделения (ответственного работника) по управлению рисками от структурного подразделения (ответственного работника) по кибербезопасности.

52. Подразделение (ответственный работник) по управлению рисками разрабатывает внутренний документ, определяющий порядок управления рисками кибербезопасности, который включает, но не ограничивается:

1) процедуры идентификации и классификации информационных активов, с целью выявления критичных информационных активов;

2) процедуры идентификации уязвимостей критичных объектов цифровой инфраструктуры информационных активов;

3) процедуры идентификации потенциальных угроз в отношении критичных информационных активов;

4) процедуры идентификации существующих мер управления рисками кибербезопасности;

5) процедуры оценки вероятности и последствий нарушения конфиденциальности, целостности и доступности информационных активов, применяя качественные и (или) количественные методы оценки, в том числе на основании данных об их реализации;

6) процедуры сбора и хранения сведений о реализации существенных рисков кибербезопасности;

7) процедуры формирования реестра рисков, включающего риски кибербезопасности;

8) процедуры мониторинга исполнения мер по обработке рисков кибербезопасности

.

Глава 12. Управление комплаенс-риском

53. Орган управления (исполнительный орган, наблюдательный совет – при наличии) ПУЦА контролирует процедуру управления комплаенс-риском ПУЦА, создает подразделение (назначает ответственного работника) по комплаенс-контролю у ПУЦА, назначает и освобождает от должности главного комплаенс-контролера, утверждает политику управления комплаенс-риском.

Подразделение (ответственный работник) по комплаенс-контролю организует процедуры для соблюдения требований гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о ПОД/ФТ/ФРОМУ, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью, законодательства иностранных государств, оказывающих влияние на деятельность ПУЦА, а также внутренних документов ПУЦА, регламентирующих порядок оказания ПУЦА услуг и проведения операций на финансовом рынке, и предоставляет полную и достоверную информацию органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА о наличии комплаенс-риска.

Подразделение (ответственный работник) по комплаенс-контролю отвечает за разработку политики управления комплаенс-риском, подлежащей утверждению органом управления (исполнительным органом, наблюдательным советом – при наличии) ПУЦА и содержащей основные принципы управления комплаенс-риском, в том числе принципы создания комплаенс-культуры у ПУЦА, на основании которых выявляется и управляется комплаенс-риск на всех уровнях структуры ПУЦА.

54. Подразделение (ответственный работник) по комплаенс-контролю является ответственным за разработку политики управления комплаенс-риском, обеспечение управления комплаенс-риском и координацию деятельности ПУЦА по управлению комплаенс-риском. Подразделение (ответственный работник) по комплаенс-контролю обеспечивает соответствие политики и процедур управления комплаенс-риском, в том числе, риском легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения (далее – ОД/ФТ/ФРОМУ), требованиям законодательства о ПОД/ФТ/ ФРОМУ.

Подразделение (ответственный работник) по комплаенс-контролю является структурным подразделением (ответственным работником) ПУЦА, независимым от

какой-либо деятельности структурных подразделений ПУЦА, составляющих первую линию защиты.

Независимость подразделения (ответственного работника) по комплаенс-контролю обеспечивается следующими факторами:

подразделение (ответственный работник) по комплаенс-контролю имеет статус самостоятельного структурного подразделения;

работники подразделения по комплаенс-контролю (ответственный работник по комплаенс-контролю) не занимают должности по совместительству в иных структурных подразделениях ПУЦА, за исключением занятия должности руководителя подразделения по управлению рисками (ответственного сотрудника по управлению рисками) и (или) подразделения по ПОД/ФТ/ФРОМУ (ответственного сотрудника по ПОД/ФТ/ФРОМУ);

руководитель и работники подразделения по комплаенс-контролю не оказываются в ситуации, когда возможен конфликт интересов между их обязанностями по управлению комплаенс-риском и любыми другими возложенными на них обязанностями;

работники подразделения по комплаенс-контролю в рамках своей компетенции имеют доступ и при необходимости требуют любую информацию у структурных подразделений ПУЦА, дочерних организаций ПУЦА, а также привлекают работников ПУЦА и его дочерних организаций для содействия выполнению функции комплаенс-контроля.

55. Подразделение (ответственный работник) по комплаенс-контролю осуществляет следующие функции (но не ограничиваясь):

1) разработку внутреннего порядка, способов и процедур выявления, измерения, мониторинга и контроля за комплаенс-риском ПУЦА на консолидированной основе;

2) разработку, внедрение и обеспечение наличия правил внутреннего контроля для целей ПОД/ФТ/ФРОМУ;

3) формирование комплаенс-программы (плана), которая включает в том числе:

проверку соблюдения подразделениями ПУЦА политики управления комплаенс-риском с учетом требований гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о ПОД/ФТ/ФРОМУ, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью;

обучение персонала по вопросам управления комплаенс-риском;

4) содействие органам ПУЦА в управлении комплаенс-риском ПУЦА;

5) консультирование руководства и работников ПУЦА о нормах гражданского и налогового законодательства Республики Казахстан, Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законодательства Республики Казахстан о государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций, о цифровых активах, о валютном регулировании и валютном контроле, о рынке ценных бумаг, о бухгалтерском учете и финансовой отчетности, о ПОД/ФТ/ФРОМУ, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью, о правилах, о политиках, имеющих отношение к управлению комплаенс-риском, включая информирование об изменениях, за исключением случаев, когда такую функцию выполняет юридическое подразделение (ответственный работник по правовому обеспечению) ПУЦА;

6) контроль организации у ПУЦА работы по ознакомлению работников ПУЦА с требованиями внутренних документов ПУЦА, регламентирующих порядок оказания ПУЦА услуг и проведения операций на рынке;

7) координацию деятельности дочерних организаций ПУЦА по вопросам управления комплаенс-риском, в том числе риском ОД/ФТ/ФРОМУ;

8) обязательное участие в процессе внедрения новых продуктов и услуг;

9) обеспечение организации в ПУЦА мероприятий по выявлению, оценке и контролю конфликтов интересов;

10) разработку процессов и процедур предотвращения нарушений требований законодательства о ПОД/ФТ/ФРОМУ, политик и процедур управления комплаенс-риском, риском ОД/ФТ/ФРОМУ (далее – комплаенс-требований);

11) разработку самостоятельно или совместно со структурными подразделениями и должностными лицами ПУЦА рекомендаций и корректирующих мер по устранению выявленных нарушений комплаенс-требований, фактов вовлечения ПУЦА, работников ПУЦА и услуг ПУЦА в противоправные действия, связанные с незаконным производством, оборотом и (или) транзитом наркотиков, организацией деятельности финансовых пирамид, осуществлением переводов денег и (или) цифровых активов в пользу электронного казино и интернет-казино, иностранных букмекерских контор и (или) тотализаторов, не имеющих лицензий на право занятия деятельностью в сфере игорного бизнеса в Республике Казахстан, и недостатков в работе ПУЦА, связанных с управлением комплаенс-риском и представление соответствующей информации органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

12) разработку и ведение системы отчетности по комплаенс-риску и предоставление на периодической основе информации по вопросам управления комплаенс-риском органу управления (исполнительному органу, наблюдательному совету – при наличии) ПУЦА;

13) разработку внутреннего порядка взаимодействия и координации работы управлению комплаенс-риском со структурными подразделениями ПУЦА, в том числе с подразделением (ответственным работником) по внутреннему аудиту;

14) координацию работы по сбору количественных и качественных показателей для оценки риска вовлеченности ПУЦА рискам ОД/ФТ/ФРОМУ и передачу информации в Национальный Банк Республики Казахстан ежегодно не позднее 5 февраля года, следующего за отчетным годом.

Главный комплаенс-контроллер (комплаенс-контроллер) несет ответственность за исполнение функций, определенных настоящим пунктом, надлежащую реализацию подразделением (ответственным работником) по комплаенс-контролю процессов и процедур по предотвращению и корректирующих мер по устранению нарушений комплаенс-требований.

Отдельные функции управления комплаенс-риском в соответствии с внутренними документами ПУЦА делегируются при необходимости иным структурным подразделениям ПУЦА, при условии отсутствия конфликта интересов.

56. Система управления комплаенс-риском включает, но не ограничивается:

1) политику и процедуры управления комплаенс-риском;

2) политику и процедуры управления риском ОД/ФТ/ФРОМУ, в том числе включающие программу принятия и обслуживания клиентов (customer acceptance policy). ПУЦА при разработке и реализации процедур принятия решения о приеме клиента на обслуживание учитывает присущие факторы риска;

3) оценку эффективности системы управления комплаенс-риском подразделением (ответственным работником) по внутреннему аудиту.

Система управления комплаенс-риском основывается на 3 (трех) линиях защиты:

работники ПУЦА;

подразделение (ответственный работник) по комплаенс-контролю;

подразделение (ответственный работник) по внутреннему аудиту.

Глава 13. Внутренний контроль

57. Система внутреннего контроля ПУЦА создается для:

1) обеспечения операционной и финансовой эффективности деятельности ПУЦА посредством проверки эффективности и рентабельности осуществления деятельности ПУЦА и определения вероятности убытков;

2) обеспечения надежности, полноты и своевременности финансовой и управленческой информации посредством проверки достоверности, и качественного составления финансовой и управленческой отчетности ПУЦА;

3) обеспечения соответствия внутренних документов, определяющих внутренние политики и процедуры ПУЦА требованиям законодательства Республики Казахстан о

цифровых активах, о рынке ценных бумаг, об акционерных обществах, о товариществах с ограниченной и дополнительной ответственностью;

4) недопущение вовлечения ПУЦА и его работников, клиентов ПУЦА осуществление противоправной деятельности, в том числе мошенничества, обмана, ОД /ФТ/ФРОМУ, незаконного производства, оборота и (или) транзита наркотиков, организацию деятельности финансовых пирамид, осуществление платежей и (или) переводов ценностей с использованием цифровых активов в пользу электронного казино и интернет-казино, а также иностранных букмекерских контор и (или) тотализаторов, не имеющих лицензий на право занятия деятельностью в сфере игорного бизнеса в Республике Казахстан.

58. Система внутреннего контроля состоит из 5 (пяти) взаимосвязанных элементов:

1) управленческий контроль;

2) выявление и оценка риска;

3) осуществление контроля и разделение полномочий;

4) информация и взаимодействие;

5) мониторинг и исправление недостатков.

59. Функционирование системы внутреннего контроля происходит по принципу непрерывного поочередного прохождения следующих трех этапов:

1) формирование системы внутреннего контроля (с учетом результатов оценки эффективности) путем включения процедур во внутренние документы ПУЦА;

2) использование в работе процедур системы внутреннего контроля, определенных внутренними документами ПУЦА;

3) проведение оценки эффективности системы внутреннего контроля.

60. Подразделение (ответственный работник) по комплаенс-контролю ПУЦА осуществляет функции по внутреннему контролю.

Глава 14. Внутренний аудит

61. Служба внутреннего аудита создается (ответственный работник по внутреннему аудиту назначается) с целью решения задач, возникающих при осуществлении органом управления (исполнительным органом, наблюдательным советом – при наличии) ПУЦА функций по обеспечению наличия и функционирования адекватной системы внутреннего контроля путем предоставления объективной оценки состояния системы внутреннего контроля и рекомендаций по их совершенствованию.

Целью внутреннего аудита является оценка адекватности и эффективности систем внутреннего контроля и управления рисками по всем аспектам деятельности ПУЦА, контроль за соблюдением внутренних правил и процедур ПУЦА, исполнением рекомендаций внутренних и внешних аудиторов, мер воздействия и требований Национального Банка Республики Казахстан, установленных в отношении осуществления деятельности ПУЦА, обеспечение своевременной и достоверной

информацией о состоянии выполнения подразделениями и работниками ПУЦА, возложенных функций и задач, а также предоставление действенных и эффективных рекомендаций по улучшению работы.

62. Руководитель и работники службы внутреннего аудита (ответственный работник по внутреннему аудиту) назначаются органом управления (исполнительным органом, наблюдательным советом – при наличии) ПУЦА и имеют доступ ко всем необходимым документам, связанным с деятельностью проверяемого подразделения (ответственного работника) ПУЦА, а также их филиалов и представительств, в том числе составляющим коммерческую и служебную тайну.

63. Требования к руководителям и работникам службы внутреннего аудита, их полномочия и система вознаграждения для них определяются органом управления (исполнительным органом, наблюдательным советом – при наличии) ПУЦА.

64. Руководитель и работники службы внутреннего аудита (ответственный работник по внутреннему аудиту) не занимают иную должность, не являются членами коллегиального органа ПУЦА и не совмещают обязанности в ПУЦА и (или) дочерних организациях ПУЦА.

Приложение к Правилам
формирования системы
управления рисками
и внутреннего контроля для
операторов обмена
необеспеченных цифровых
активов, операторов
платформы цифровых
финансовых активов,
операторов торговой
платформы цифровых активов

Отчет об оценке выполнения требований к системе управления рисками

_____

(наименование оператора обмена необеспеченных цифровых активов, оператора платформы цифровых финансовых активов, оператора торговой платформы цифровых активов (далее – провайдер услуг цифровых активов)

Отчетный период: за "_____" год

№	Указание соответствующего абзаца, части, подпункта, пункта Правил	Оценка соответствия требованиям Правил	Выявленные недостатки	Принятые (планируемые) мероприятия по устранению недостатков (содержание мероприятия, сроки исполнения)	Ответственные исполнители (фамилия, имя, отчество (при его наличии), должность, контактная информация)
1	2	3	4	5	6

Общая оценка соответствия требованиям к системе управления рисками: _____

Пояснение по заполнению формы

Оценка соответствия требованиям к системе управления рисками осуществляется по трехбалльной системе следующих критериев (соответствует, частично соответствует , не соответствует):

1) оценка "соответствует" выносится при выполнении провайдером услуг цифровых активов критерия требования к системе управления рисками без каких-либо значительных недостатков;

2) оценка "частично соответствует" выносится при обнаружении недостатков, которые не считаются достаточными для появления серьезных сомнений относительно способности провайдера услуг цифровых активов в достижении соблюдения конкретного критерия требования к системе управления рисками;

3) оценка "не соответствует" выносится при невыполнении провайдером услуг цифровых активов критерия требований к системе управления рисками.

В случае, если отдельные требования к системе управления рисками не применяются в отношении провайдера услуг цифровых активов, оценка соответствия данному критерию требования не осуществляется и отмечается соответствующей записью "не применимо".