УТВЕРЖДЕНО

Решение Наблюдательного совета Парка высоких технологий

(протокол от 29.06.2026 № 3)

ПОЛОЖЕНИЕ
о требованиях к правилам внутреннего контроля криптобанков

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящим Положением установлены требования к правилам внутреннего контроля криптобанков, являющихся резидентами Парка высоких технологий (далее – ПВТ) и осуществляющих иную деятельность с использованием цифровых знаков (токенов), в том числе содержащую признаки профессиональной и биржевой деятельности по ценным бумагам, деятельности инвестиционного фонда, секьюритизации, а также осуществление операций по созданию и размещению собственных цифровых знаков (токенов), совмещенную с совершением банковских, платежных и иных связанных с ними финансовых операций в соответствии с Положением о порядке осуществления криптобанками деятельности с использованием цифровых знаков (токенов), утвержденным решением Наблюдательного совета Парка высоких технологий (протокол от 15 апреля 2026 г. № 2), в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения (далее – правила внутреннего контроля).

2. Применительно к настоящему Положению нижеприведенные термины используются в следующих значениях:

агенты по идентификации – лица, осуществляющие идентификацию клиентов криптобанка, их представителей по поручению криптобанка на основании договора или законодательного акта;

анализируемый период – отрезок времени, в среднем составляющий один календарный месяц, определяемый криптобанком в зависимости от вида осуществляемых клиентом финансовых операций, за который криптобанк анализирует финансовые операции клиента на стадии последующего контроля;

анкета клиента – совокупность данных в электронном виде, собранных криптобанком в отношении клиента в ходе его идентификации и верификации, содержащих сведения о клиенте и его деятельности, установленные статьей 8 Закона Республики Беларусь от 30 июня 2014 г. № 165-З ”О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения“ (далее – Закон № 165-З), настоящим Положением и правилами внутреннего контроля криптобанка, а также иную информацию, необходимую для применения расширенных мер внутреннего контроля по идентификации клиентов, их представителей;

анкетирование – составление криптобанком анкеты клиента;

банк – банк, небанковская кредитно-финансовая организация, открытое акционерное общество ”Банк развития Республики Беларусь“;

банк-корреспондент – банк, в котором криптобанком открыт корреспондентский счет и (или) иной счет криптобанка-респондента;

банк-респондент – банк, открывший корреспондентский и (или) иной счет в криптобанке;

криптобанк-корреспондент – криптобанк, в котором открыт корреспондентский счет и (или) иной счет банка-респондента, криптобанка-респондента;

криптобанк-респондент – криптобанк, открывший корреспондентский счет и (или) иной счет в банке, криптобанке;

клиент, осуществляющий разовую операцию, – лицо, за исключением банка-респондента и криптобанка-респондента, осуществляющее финансовую операцию без заключенного договора на осуществление финансовых операций в письменной форме, включая договор, заключенный в электронном виде без использования электронной цифровой подписи в случаях, предусмотренных законодательными актами;

корреспондентские отношения – предоставление услуг (продуктов) в рамках договорных отношений между криптобанками, банком и криптобанком;

неоднократное осуществление финансовых операций – осуществление клиентом криптобанка финансовых операций два и более раза в течение анализируемого периода;

однотипные финансовые операции – финансовые операции, соответствующие одному признаку подозрительности финансовых операций и выявляемые по результатам мониторинга финансовых операций клиента на стадии последующего контроля;

оператор зарубежной торговой площадки – нерезидент Республики Беларусь, который осуществляет деятельность, аналогичную деятельности

оператора криптоплатформы, в соответствии с законодательством иностранного государства;

организация – организация-резидент Республики Беларусь, организация-нерезидент Республики Беларусь, в том числе организация, не являющаяся юридическим лицом;

подозрительная финансовая операция – финансовая операция, в отношении которой у криптобанка возникли подозрения, что она осуществляется в целях получения и (или) легализации доходов, полученных преступным путем, финансирования террористической деятельности, распространения или финансирования распространения оружия массового поражения, после принятия криптобанком решения об отнесении ее к финансовой операции, подлежащей особому контролю;

представитель клиента – лицо, осуществляющее финансовые операции от имени клиента криптобанка, полномочия которого подтверждены в порядке, определенном законодательством, либо явствуют из обстановки, в которой действует представитель;

систематическое осуществление финансовых операций – осуществление клиентом криптобанка финансовых операций три и более раз в течение анализируемого периода;

финансовая операция, вызывающая подозрение, – финансовая операция, в отношении которой у криптобанка возникли подозрения, что она осуществляется в целях получения и (или) легализации доходов, полученных преступным путем, финансирования террористической деятельности, распространения или финансирования распространения оружия массового поражения, до принятия криптобанком решения об отнесении (не отнесении) ее к финансовой операции, подлежащей особому контролю.

Термин ”платежная операция“ используется в значении, определенном подпунктом 1.19 пункта 1 статьи 2 Закона Республики Беларусь от 19 апреля 2022 г. № 164-З ”О платежных системах и платежных услугах“.

Термин ”цифровой знак (токен)“ используется в значении, определенном пунктом 12 приложения 1 к Декрету Президента Республики Беларусь от 21 декабря 2017 г. № 8 ”О развитии цифровой экономики“ (далее – Декрет № 8).

Термины ”бенефициарный владелец“, ”блокирование финансовой операции“, ”верификация“, ”внутренний контроль“, ”выгодоприобретатель“, ”замораживание средств“, ”идентификация“, ”клиент“, ”легализация доходов, полученных преступным путем“, ”обновление (актуализация)“, ”организация, не являющаяся юридическим лицом“, ”средства“, ”сумма финансовой операции“, ”участник финансовой операции“, ”финансирование распространения оружия массового поражения, ”финансовая операция“ используются в значениях,

определенных соответственно абзацами вторым-шестым, девятым-двенадцатым, четырнадцатым, пятнадцатым, восемнадцатым-двадцать вторым части первой статьи 1 Закона № 165-З.

Термин ”комплаенс-контроль“ используется в значении, определенном абзацем восьмым части первой пункта 2 Инструкции об организации корпоративного управления, утвержденной постановлением Правления Национального банка Республики Беларусь от 21 февраля 2024 г. № 62.

ГЛАВА 2
ОРГАНИЗАЦИЯ СИСТЕМЫ ВНУТРЕННЕГО КОНТРОЛЯ В СФЕРЕ ПРЕДОТВРАЩЕНИЯ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, ФИНАНСИРОВАНИЯ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ И ФИНАНСИРОВАНИЯ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ

3. Система внутреннего контроля криптобанка в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения (далее – ПОД/ФТ) организуется в рамках системы внутреннего контроля криптобанка и системы управления рисками криптобанка и должна обеспечивать недопущение умышленного или невольного вовлечения криптобанка в процесс легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения.

4.Криптобанк разрабатывает правила внутреннего контроля с учетом особенностей своей организационной структуры, характера и объема осуществляемых финансовых операций с цифровыми знаками (токенами) и банковских операций, а также уровня рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения.

При разработке правил внутреннего контроля при осуществлении финансовых операций криптобанк руководствуется требованиями настоящего Положения с учетом масштабов деятельности, состава и объема осуществляемых банковских операций и операций с цифровыми знаками (токенами).

Правила внутреннего контроля утверждаются исполнительным органом криптобанка.

5. Правила внутреннего контроля криптобанка включают процедуры и порядки, предусмотренные частью третьей статьи 5 Закона № 165-З.

Дополнительно правила внутреннего контроля криптобанка должны включать:

критерии выявления и признаки подозрительных финансовых операций, которые могут являться основаниями для отказа в осуществлении финансовой операции с учетом особенностей деятельности криптобанка;

порядок информирования клиента о приостановлении криптобанком финансовой операции и (или) об отказе в ее осуществлении, об отказе в подключении клиента к системе дистанционного обслуживания, о прекращении или приостановлении оказания услуг посредством такой системы, об отказе в одностороннем порядке от исполнения договора на осуществление финансовых операций в письменной форме;

перечень мер, принимаемых для проверки представленной клиентами информации об источниках происхождения их средств, а также зависимость характера данных мер от цены сделки (размера операции в денежном выражении) и иных факторов;

порядок применения мер внутреннего контроля при приобретении или отчуждении клиентом цифровых знаков (токенов) в течение календарного месяца на общую сумму, не превышающую 2000 базовых величин.

6. Система внутреннего контроля криптобанка в сфере ПОД/ФТ реализуется по следующим основным направлениям:

идентификация и верификация в случаях, предусмотренных законодательством, клиентов криптобанка, осуществляющих финансовые операции, мониторинг их деятельности в процессе обслуживания;

выявление, документальное фиксирование финансовой операции, подлежащей особому контролю, и передача соответствующих сведений в орган финансового мониторинга;

замораживание средств и (или) блокирование финансовых операций лиц, причастных к террористической деятельности;

хранение сведений и документов (их копий) в течение срока, установленного законодательством.

7. Порядок применения мер внутреннего контроля криптобанком, предусмотренный в правилах внутреннего контроля, должен обеспечивать недопущение его вовлечения в процесс легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения.

8. Внутренний контроль проводится на всех стадиях осуществления финансовых операций и подразделяется на:

предварительный контроль, проводимый путем сбора и изучения необходимых сведений и документов (их копий, изображений) и фиксирования данных в анкете клиента для формирования представления о клиенте;

текущий контроль, проводимый путем мониторинга финансовых операций, осуществляемых клиентом, с учетом сведений, имеющихся у криптобанка, после проведения предварительного контроля, с целью выявления финансовых операций, подлежащих особому контролю;

последующий контроль, проводимый путем анализа осуществленных за предыдущий период финансовых операций клиента с целью выявления подозрительных финансовых операций, носящих длительный характер и не определяемых на стадии текущего контроля как подлежащих особому контролю.

9. Криптобанк в соответствии с требованиями постановления Правления Национального банка Республики Беларусь от 21 февраля 2024 г. № 62 ”Об организации корпоративного управления“ создает подразделение комплаенс-контроля, включающее функции по ПОД/ФТ.

Функции подразделения комплаенс-контроля определены в пункте 8 Инструкции о требованиях к правилам внутреннего контроля в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения при осуществлении банковских операций, утвержденной постановлением Правления Национального банка Республики Беларусь от 24 декабря 2014 г. № 818 (далее – Инструкция №818).

Криптобанки уведомляют Национальный банк о назначении руководителя подразделения комплаенс-контроля, его заместителя (лиц, их замещающих) в соответствии с пунктом 10 Инструкции № 818.

Криптобанк уведомляет Секретариат Наблюдательного совета Парка высоких технологий о назначении, смене руководителя подразделения комплаенс-контроля, его заместителя в течение пяти рабочих дней со дня принятия соответствующего приказа с представлением по нему сведений по форме согласно приложению 1 посредством использования системы межведомственного электронного документооборота государственных органов (далее – СМДО). В случае невозможности направления по техническим причинам сведений посредством СМДО они направляются на бумажном носителе заказным письмом.

10. Локальным правовым актом криптобанка назначается(ются) ответственное(ые) должностное(ые) лицо(а), в обязанности которого входит выполнение следующих функций:

организация проведения идентификации участников финансовой операции, верификации и обновления (актуализации) данных о клиентах криптобанка, определения источников происхождения средств клиентов;

принятие мотивированного решения о присвоении работе с клиентом иной итоговой степени риска;

принятие решения о признании финансовой операции подозрительной (неподозрительной) и представлении (непредставлении) сведений о ней в орган финансового мониторинга;

принятие решения о приостановлении (возобновлении) финансовой операции в соответствии с законодательными актами и настоящим Положением;

принятие решения об отказе в осуществлении финансовой операции в соответствии с законодательными актами и настоящим Положением;

принятие решения об отказе от исполнения договора на осуществление финансовых операций в письменной форме в случаях, предусмотренных законодательными актами;

принятие решения об отказе в подключении клиента к системе дистанционного обслуживания, прекращении или приостановлении оказания услуг посредством такой системы в случаях, предусмотренных законодательными актами;

принятие решения о замораживании средств и (или) блокировании финансовой операции в отношении лиц, включенных в перечень организаций и физических лиц, в том числе индивидуальных предпринимателей, причастных к террористической деятельности (далее – перечень), решения об отмене соответствующих мер, в случаях, предусмотренных законодательными актами;

принятие решения об отнесении услуг (продуктов) криптобанка к высокой степени риска;

получение и обновление перечня;

получение реестра адресов (идентификаторов) виртуальных кошельков, использовавшихся (используемых) для осуществления противоправной деятельности, направляемого Секретариатом Наблюдательного совета ПВТ в соответствии с Положением о порядке ведения и применения реестра адресов (идентификаторов) виртуальных кошельков, использовавшихся (используемых) для осуществления противоправной деятельности, утвержденным Указом Президента Республики Беларусь от 14 февраля 2022 г. № 48, и поддержание в актуальном состоянии сведений об адресах (идентификаторах) виртуальных кошельков, внесенных в названный реестр (исключенных из него);

обеспечение проверки правильности и полноты заполнения специальных формуляров регистрации финансовых операций, подлежащих особому контролю (далее – специальный формуляр), в соответствии с Инструкцией о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю, утвержденной постановлением Совета Министров Республики Беларусь от 16 марта

2006 г. № 367, а также своевременности их представления в орган финансового мониторинга;

организация последующего контроля с целью выявления подозрительных финансовых операций, носящих длительный характер и не определяемых на стадии текущего контроля как подлежащих особому контролю;

подписание электронной цифровой подписью отправляемых в орган финансового мониторинга специальных формуляров в виде электронного документа;

проверка знаний работников структурных подразделений криптобанка, входящих в организационную структуру системы внутреннего контроля в сфере ПОД/ФТ;

иные функции, предусмотренные правилами внутреннего контроля криптобанка и законодательством в сфере ПОД/ФТ.

Выполнение функций, указанных в части первой настоящего пункта, может быть возложено на одного или нескольких ответственных должностных лиц из числа руководителей (заместителей руководителей) обособленных и иных структурных подразделений криптобанка, работников подразделения комплаенс-контроля. Принятие решений, указанных в абзацах шестом и девятом части первой настоящего пункта, на период отсутствия должностного лица (нерабочее время, выходные и праздничные дни) может быть возложено на иное уполномоченное лицо.

11. Должностным лицом, ответственным за выполнение правил внутреннего контроля, назначается руководитель криптобанка или его заместитель в соответствии с приказом руководителя криптобанка.

12. При определении обязанностей работников подразделений криптобанка, входящих в организационную структуру системы внутреннего контроля криптобанка, криптобанк руководствуется следующим.

Лицо, непосредственно осуществившее финансовую операцию, лицо, в обязанности которого входит осуществление последующего внутреннего контроля и (или) лицо, в обязанности которого входит выявление среди клиентов криптобанка лиц, в отношении которых должны быть применены меры по замораживанию средств и (или) блокированию финансовых операций, являются лицами, ответственными за составление сообщения, предусмотренного пунктом 87 настоящего Положения. Выявление среди клиентов криптобанка лиц, в отношении которых должны быть применены меры по замораживанию средств и (или) блокированию финансовых операций, может быть возложено на ответственное должностное лицо.

Ответственное должностное лицо, в обязанности которого входит проверка правильности и полноты заполнения специального формуляра, и ответственное должностное лицо, принявшее решение о признании

финансовой операции клиента подозрительной и представлении сведений о ней в орган финансового мониторинга, являются лицами, ответственными за соблюдение порядка заполнения специального формуляра.

Лица, непосредственно осуществившие идентификацию и (или) анкетирование клиента, верификацию данных о клиенте, и руководители подразделений, в функции которых входит проведение идентификации и (или) анкетирования клиентов, верификации данных о клиенте, являются лицами, ответственными за соблюдение порядка идентификации и (или) анкетирования клиентов, верификации данных о клиентах криптобанка.

Криптобанк не вправе назначать ответственным за соблюдение порядка заполнения специального формуляра лицо, составившее по такой операции сообщение, предусмотренное пунктом 87 настоящего Положения.

Распределение обязанностей работников криптобанка в части выполнения мер по ПОД/ФТ должно быть закреплено в локальных правовых актах криптобанка.

ГЛАВА 3
УПРАВЛЕНИЕ РИСКАМИ, СВЯЗАННЫМИ С ЛЕГАЛИЗАЦИЕЙ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, ФИНАНСИРОВАНИЕМ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ И ФИНАНСИРОВАНИЕМ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ

13. Криптобанк в целях управления рисками, связанными с легализацией доходов, полученных преступным путем, финансирование террористической деятельности и финансирование распространения оружия массового поражения, осуществляет процедуры управления (выявления, оценки, мониторинга, контроля, ограничения (снижения) рисками, связанными с легализацией доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, с учетом риск-ориентированного подхода в соответствии со статьей 5 Закона № 165-З и постановлением Совета Министров Республики Беларусь от 24 декабря 2014 г. № 1249 ”Об установлении общих требований к правилам внутреннего контроля“ (далее – постановление № 1249), а также в соответствии с требованиями настоящего Положения.

14. Криптобанк систематически, но не реже одного раза в три года осуществляет внутреннюю оценку рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения (далее – внутренняя оценка рисков). При необходимости оценка областей деятельности криптобанка повышенного

риска, в том числе механизмов внутреннего контроля, может проводиться чаще одного раза в три года.

Для организации проведения внутренней оценки рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, криптобанк разрабатывает методологию проведения оценки, включая периодичность и основания для оценки рисков отдельных областей деятельности криптобанка и конкретных механизмов внутреннего контроля, способ ее проведения.

При проведении внутренней оценки рисков криптобанк анализирует следующую информацию:

материалы международных и национальных конференций, семинаров, совещаний по вопросам противодействия легализации доходов, полученных преступным путем, финансированию террористической деятельности и финансированию распространения оружия массового поражения;

отчеты, информацию, руководства международных организаций, включая информацию, размещенную на сайтах Группы разработки финансовых мер борьбы с отмыванием денег (далее – ФАТФ) и Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма в глобальной компьютерной сети Интернет;

материалы национальной и (или) секторальной оценки рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, в банковском секторе и секторе организаций в сфере оборота цифровых знаков (токенов) и рисков, возникающих в результате деятельности, связанной с цифровыми знаками (токенами), а также деятельности и операций, осуществляемых соответствующими резидентами ПВТ с цифровыми знаками (токенами);

характерные для деятельности криптобанка риски, связанные с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения.

Криптобанк обеспечивает документирование результатов внутренней оценки рисков, выполняет сопоставление текущей оценки с результатами предыдущей оценки, определяет план действий по ограничению (снижению) рисков высокой степени, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, назначает ответственных лиц и устанавливает сроки выполнения плана.

Документальное фиксирование результатов внутренней оценки рисков осуществляется в отчете о внутренней оценке рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, включающем сведения по перечню согласно приложению 2, который утверждает должностное лицо, ответственное за выполнение правил внутреннего контроля.

При оценке отдельных областей деятельности криптобанка повышенного риска, в том числе механизмов внутреннего контроля, отчет утверждается в порядке, определенном правилами внутреннего контроля, и содержит объем сведений, которые характеризуют оцениваемую область.

15. При реализации процедуры управления рисками, связанными с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, криптобанк принимает меры по определению, классификации, описанию и оценке рисков с учетом факторов риска, влияющих на повышение (понижение) степени рисков.

16. Риск работы с клиентом оценивается криптобанком по шкале рисков, которая состоит из трех степеней (низкая, средняя и высокая).

17. Для оценки риска работы с клиентом криптобанк использует трехвекторную модель распределения рисков, в рамках которой оцениваются следующие векторы:

риск по профилю клиента;

риск по географическому региону;

риск по видам операций.

18. При оценке вектора ”риск по профилю клиента“ банком учитывается присвоенная в соответствии с пунктом 36 настоящего Положения категория клиента и анализируется следующая информация:

18.1. основные виды деятельности клиента (для физических лиц - место работы, занимаемая должность);

18.2. сведения о постоянных контрагентах клиента и их деловой репутации;

18.3. отнесение клиента к лицам, работа с которыми изначально сопряжена с факторами, повышающими (понижающими) степень риска;

18.4. сведения о лицах, способных прямо и (или) косвенно (через иных лиц) определять (оказывать влияние на принятие) решения клиента, о лицах, на принятие решений которыми клиент оказывает такое влияние, а также о деловой репутации этих лиц (для физических лиц и индивидуальных предпринимателей);

18.5. сведения об учредителях (участниках), бенефициарных владельцах, лицах, которые имеют право давать обязательные указания

либо иным образом имеют возможность определять действия клиента, а также об их деловой репутации (для организаций и банков-респондентов);

18.6. сведения о руководителе, главном бухгалтере и (или) иных уполномоченных должностных лицах, которым в установленном порядке предоставлено право действовать от имени клиента, а также об их деловой репутации (для организаций и банков-респондентов);

18.7. полнота представленных клиентом идентификационных данных, а также их соответствие имеющейся в криптобанке информации, полученной в результате верификации;

18.8. сведения о деловой репутации клиента;

18.9. иные сведения, которые криптобанк считает необходимыми для включения в анализ.

19. При оценке вектора ”риск по географическому региону“ криптобанком анализируется следующая информация:

19.1. признак резидентства клиента;

19.2. государство (территория) регистрации, место жительства или нахождения клиента;

19.3. государство (территория) регистрации, место жительства или нахождения лиц, способных прямо и (или) косвенно (через иных лиц) определять (оказывать влияние на принятие) решения клиента, а также сведения о государствах (территориях) регистрации, жительства или нахождения лиц, на принятие решений, которыми клиент оказывает такое влияние;

19.4. география бизнеса клиента (государства (территории), в которых открыты счета, и государства (территории) регистрации постоянных контрагентов клиента);

19.5. иные сведения, которые криптобанк считает необходимыми для включения в анализ.

20. При оценке вектора ”риск по видам операций“ криптобанком анализируется следующая информация:

20.1. соответствие осуществляемых клиентом финансовых операций его основным видам деятельности;

20.2. условия и виды финансовых операций, осуществляемых клиентом на постоянной основе, а также их соответствие факторам, повышающим (понижающим) степень риска;

20.3. способ оказания услуг (реализации продуктов) клиентам;

20.4. финансовые операции, подлежащие особому контролю, осуществленные клиентом за анализируемый период;

20.5. факты приостановления финансовых операций по счету по постановлению (решению) уполномоченных государственных органов (должностных лиц) или наложения ареста на денежные средства, цифровые знаки (токены), находящиеся на счете и криптоаккаунте клиента;

20.6. принятые решения об отказе и (или) приостановлении финансовых операций, о прекращении договорных отношений с клиентом, в том числе по договорам, предусматривающим оказание клиенту дополнительных услуг посредством систем дистанционного обслуживания;

20.7. иные сведения, которые криптобанк считает необходимыми для включения в анализ.

21. К клиентам, работа с которыми при оценке вектора ”риск по профилю клиента“ сопряжена с факторами, повышающими степень риска, относятся:

21.1. организация, физическое лицо, в том числе индивидуальный предприниматель, включенные в перечень;

21.2. иностранные публичные должностные лица, должностные лица публичных международных организаций, лица, занимающие должности, включенные в определяемый Президентом Республики Беларусь перечень государственных должностей Республики Беларусь члены их семей и приближенные к ним лица (далее – публичные должностные лица);

21.3. организации, бенефициарным владельцем которых является лицо, указанное в подпунктах 21.1 и 21.2 настоящего пункта;

21.4. клиенты, контрагентом которых является лицо, указанное в подпунктах 21.1 и 21.2 настоящего пункта;

21.5. организации, собственник имущества, учредители (участники) и (или) руководители которых привлекались к уголовной ответственности (при наличии у криптобанка данной информации);

21.6. клиенты, в отношении которых имеется негативная информация, в том числе полученная от государственных органов;

21.7 организации, в которых учредителем (участником), руководителем и (или) главным бухгалтером одновременно является одно физическое лицо;

21.8. учредители (участники) и (или) руководители организации, индивидуальный предприниматель, которые были связаны с клиентами банка, имеющими негативную деловую репутацию;

21.9. клиенты, с которыми невозможно в течение более чем 30 дней установить связь по указанным ими контактным данным;

21.10. организации, информация о деятельности которых не найдена в глобальной компьютерной сети Интернет;

21.11. клиенты, которые систематически без уважительной причины (немотивированно) избегают установления видеосвязи с криптобанком в случае предложения установить контакт таким образом;

21.12. физические лица, которые взаимодействуют с криптобанком исключительно через представителя, действующего на основании доверенности;

21.13. организации, основная деятельность которых связана с благотворительностью;

21.14. организации, основным видом деятельности которых является купля и продажа недвижимого имущества и оказание посреднических услуг при совершении сделок с недвижимым имуществом;

21.15. организации, занимающиеся туристической деятельностью;

21.16. организации, деятельность которых связана с интенсивным оборотом наличных денежных средств, в том числе с оказанием услуг в сфере розничной торговли, общественного питания;

21.17. организации, деятельность которых связана с реализацией (в том числе комиссионной) предметов искусства, антиквариата, легковых транспортных средств;

21.18. организации, деятельность которых связана с реализацией драгоценных металлов, драгоценных камней, а также ювелирных изделий, содержащих драгоценные металлы и драгоценные камни, за исключением таких финансовых операций, проводимых банками;

21.19. организации, деятельность которых связана с предоставлением услуг интернет-платформ (краудфандинг, краудлендинг, краудинвестинг) в качестве инструмента взаимодействия потребителей и производителей товаров и услуг, инвесторов и соискателей инвестиций;

21.20. организации, деятельность которых связана с производством оружия, или посредническая деятельность клиента по реализации оружия;

21.21. организации, осуществляющие деятельность в сфере игорного бизнеса;

21.22. организации, в которых руководитель, главный бухгалтер и (или) иные уполномоченные должностные лица, которым в установленном порядке предоставлено право действовать от имени организации, являются учредителями (участниками) других организаций с долей в уставном фонде более 25 процентов или собственниками других организаций;

21.23. организации, в которых учредители (участники), имеющие долю в уставном фонде более 25 процентов, или собственники являются учредителями (участниками), имеющими долю в уставном фонде более 25 процентов, руководителями или собственниками других организаций;

21.24. иные лица, определяемые криптобанком.

22. К клиентам, работа с которыми при оценке вектора ”риск по профилю клиента“ сопряжена с факторами, понижающими степень риска, относятся:

22.1. государственные органы и государственные организации Республики Беларусь;

22.2. клиенты, период договорных отношений криптобанка с которыми составляет более одного года, при условии, что у криптобанка

не имеется информации о наличии в отношении данных клиентов факторов, повышающих степень риска;

22.3. иные лица, определяемые криптобанком.

23. К клиентам, работа с которыми при оценке вектора ”риск по географическому региону“ сопряжена с факторами, повышающими степень риска, относятся:

23.1. лица, зарегистрированные, имеющие место жительства или место нахождения в государстве (на территории), которое (которая) не выполняет рекомендации ФАТФ, не участвует в международном сотрудничестве в сфере ПОД/ФТ, либо лица, о которых имеются сведения об осуществлении финансовых операций через счета в банке, небанковской кредитно-финансовой организации, зарегистрированных в таком государстве (на такой территории);

23.2. лица, зарегистрированные, имеющие место жительства или место нахождения в государстве (территории), которое включено в перечень оффшорных зон - государств (территорий), в которых действует льготный налоговый режим и (или) не предусматривается раскрытие и предоставление информации о финансовых операциях, утвержденный Указом Президента Республики Беларусь от 25 мая 2006 г. № 353 (далее – оффшорная зона);

23.3. организации, учредителем, бенефициарным владельцем которых является лицо, указанное в подпунктах 23.1 и 23.2 настоящего пункта;

23.4. клиенты, постоянными контрагентами которых являются лица, указанные в подпунктах 23.1 и 23.2 настоящего пункта;

23.5. иные лица, определяемые криптобанком.

24. К клиентам, работа с которыми при оценке вектора ”риск по географическому региону“ сопряжена с факторами, понижающими степень риска, относятся:

24.1. резиденты Республики Беларусь;

24.2. иные лица, определяемые криптобанком.

25. При оценке вектора ”риск по видам операций“ к факторам, повышающим степень риска, относятся:

25.1. систематически осуществляемые клиентом подозрительные финансовые операции;

25.2. приостановление финансовых операций по постановлению (решению) уполномоченных государственных органов (должностных лиц) или наложение ареста на денежные средства, находящиеся на счете клиента, или цифровые знаки (токены), находящиеся на криптоаккаунте клиента (данный фактор не применяется в случаях, если с момента приостановления финансовых операций или наложения ареста прошло более трех лет);

25.3. негативная оценка криптобанком мер, принимаемых клиентом из числа лиц, осуществляющих финансовые операции, в целях ПОД/ФТ;

25.4. открытие клиенту счета и/или криптоаккаунта по доверенности лицом, не являющимся работником клиента;

25.5. финансовые операции, проводимые через счета, открытые в оффшорных зонах;

25.6. операции клиента с цифровыми знаками (токенами), контрагентами по которым являются юридические лица, не имеющие специальное разрешение (лицензию) или иной разрешительный документ, выданный компетентными органами (компетентными организациями) стран, в которых данные юридические лица учреждены и фактически находятся, и предусматривающий право на совершение сделок (операций) с цифровыми знаками (токенами);

25.7. принятые криптобанком в отношении данного клиента решения об отказе в осуществлении финансовых операций, о прекращении договорных отношений с клиентом;

25.8. случаи, когда клиент, являющийся организацией, с даты регистрации которой прошло менее одного календарного месяца, испрашивает совершение финансовой операции на сумму 1000 базовых величин и более;

25.9. несоответствие финансовой операции виду деятельности клиента, являющегося некоммерческой организацией;

25.10. иные факторы, определяемые криптобанком.

26. При оценке вектора ”риск по видам операций“ к факторам, понижающим степень риска, относятся:

26.1. отсутствие в течение года осуществляемых клиентом подозрительных финансовых операций;

26.2 размещение физическими лицами цифровых знаков (токенов) в криптовклады в криптобанке;

26.3 операции по расчетам в форме криптогарантий, по модели счета эскроу в цифровых знаках (токенах);

26.4. иные факторы, определяемые криптобанком.

27. В результате анализа информации о клиенте, которой располагает криптобанк, каждому из трех векторов присваивается степень риска. На основе присвоенного значения криптобанк для присвоения работе с клиентом итоговой степени риска руководствуется матрицей присвоения работе с клиентом итоговой степени риска на основе трехвекторной модели распределения рисков согласно приложению 3.

Криптобанком в правилах внутреннего контроля должен быть предусмотрен механизм определения итоговой степени риска работы с клиентом по каждому из векторов трехвекторной модели распределения рисков с учетом всех выявленных в отношении клиента факторов,

повышающих (понижающих) степень риска (с использованием балльной шкалы или иным образом).

При необходимости ответственное должностное лицо принимает в письменной форме мотивированное решение о присвоении работе с клиентом иной итоговой степени риска. Данное решение фиксируется в аналитическом разделе ”Служебная информация“ анкеты клиента.

Присвоенная криптобанком степень риска работы с клиентом (итоговая и по каждому вектору модели) указывается в аналитическом разделе ”Служебная информация“ анкеты клиента. В случае присвоения работе с клиентом высокой степени риска в рамках любого из векторов модели в разделе ”Служебная информация“ анкеты клиента указывается обоснование присвоения указанной степени риска. В качестве обоснования, криптобанк указывает соответствующие факторы, повышающие степень риска, определенные в пунктах 21, 23 и 25 настоящего Положения, либо мотивированное суждение ответственного должностного лица криптобанка, содержащее описание причины установления высокой степени риска.

28. Криптобанк при необходимости пересматривает итоговую степень риска работы с клиентом по мере изменения указанных в анкете клиента данных, в том числе полученных в результате верификации, а также характера проводимых клиентом финансовых операций.

29. Криптобанки в правилах внутреннего контроля вправе конкретизировать и дополнять факторы, предусмотренные пунктами 21 - 26 настоящего Положения.

30. Криптобанк уведомляет Секретариат Наблюдательного совета ПВТ и Национальный банк об установлении в правилах внутреннего контроля:

дополнительных сведений, которые криптобанк считает необходимыми для включения в анализ при оценке векторов ”риск по профилю клиента“, ”риск по видам операций“, ”риск по географическому региону“ согласно пунктам 18 - 20 настоящего Положения;

иных лиц, работа с которыми при оценке вектора ”риск по профилю клиента“ изначально сопряжена с факторами, повышающими (понижающими) степень риска, согласно пунктам 21 и 22 настоящего Положения;

иных лиц, работа с которыми при оценке вектора ”риск по географическому региону“ изначально сопряжена с факторами, повышающими (понижающими) степень риска, согласно пунктам 23 и 24 настоящего Положения;

дополнительных факторов, повышающих (понижающих) степень риска финансовых операций, согласно пунктам 25 и 26 настоящего Положения.

Сведения, указанные в части первой настоящего пункта, представляются криптобанком в течение пяти рабочих дней со дня утверждения правил внутреннего контроля (внесения изменений в них).

31. Криптобанк оценивает риск использования клиентами услуг (продуктов) в целях легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения (далее – риск услуги (продукта) по трехуровневой шкале рисков (низкий, средний и высокий).

Оценка риска услуги (продукта), предоставляемой криптобанком, осуществляется до внедрения новых услуг (продуктов), изменения существенных условий или способов оказания услуг (продуктов), внедрения новых технологий для осуществления финансовых операций.

Актуализация степени риска услуг (продуктов) осуществляется по мере необходимости, но не реже одного раза в год.

32. При оценке риска услуги (продукта) к факторам, повышающим степень риска услуги (продукта), относятся:

дистанционный способ оказания услуг;

использование услуг третьих сторон для реализации услуги (продукта);

отсутствие технической возможности для реализации лимитной политики;

использование новых или развивающихся технологий, которые потенциально благоприятствуют быстрому осуществлению финансовых операций или осуществлению анонимных финансовых операций;

осуществление значительного количества финансовых операций, размер которых определяется криптобанком;

осуществление финансовых операций в значительных суммах, размер которых определяется криптобанком;

выявление фактов использования клиентами услуги (продукта), предоставляемой криптобанком, в целях легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;

иные факторы, определяемые криптобанком.

33. При оценке риска услуги (продукта) к факторам, понижающим степень риска услуги (продукта), относятся:

отсутствие возможности осуществления анонимных финансовых операций;

осуществление незначительного количества финансовых операций, размер которых определяется криптобанком;

осуществление финансовых операций в незначительных суммах, размер которых определяется криптобанком;

достаточность и сформированность контрольных процедур;

иные факторы, определяемые криптобанком.

Криптобанк самостоятельно определяет в правилах внутреннего контроля критерий значительности финансовых операций.

34. Оценка риска услуг (продуктов) осуществляется с учетом следующих особенностей:

учитываются все присущие факторы, повышающие (понижающие) степень риска услуги (продукта);

каждому фактору устанавливаются оценка или весовой коэффициент, отражающие уровень риска, связанного с этим фактором, и его значимость в сравнении с прочими факторами в соответствии с разработанной криптобанком методикой;

услуге (продукту) не может быть присвоена низкая степень риска вне зависимости от сформированности контрольных процедур, если по итогам национальной, региональной, секторальной в соответствующей области деятельности оценок рисков установлено, что данная услуга (продукт) использовалась в схемах получения и (или) легализации доходов, полученных преступным путем.

Криптобанк формирует реестр рисков услуг (продуктов) в электронном виде с возможностью его вывода на печать. В реестре указываются наименование услуги (продукта), способ оказания услуги клиенту, набор факторов, используемых при анализе услуг (продуктов) криптобанка, степень присущего риска, меры по контролю и ограничению (снижению) высокого риска, а также степень остаточного риска после принятия мер. Присвоение услугам (продуктам) степени риска может осуществляться по группам клиентов, суммам финансовых операций и иным параметрам.

35. В целях осуществления контроля за рисками, связанными с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, криптобанк устанавливает адекватную систему критериев выявления и признаков подозрительных финансовых операций. Показателями ее адекватности являются:

соотношение количества представленных специальных формуляров по финансовым операциям, одним из условий особого контроля которых является условие, указанное в абзаце втором части первой статьи 7 Закона № 165-З, к количеству сообщений, составленных в соответствии с пунктом 87 настоящего Положения (в расчет не включаются специальные формуляры, по которым были представлены заменяющие специальные формуляры). Система считается адекватной, если этот показатель превышает 75 процентов;

наличие (отсутствие) документально зафиксированных фактов признания подозрительными финансовых операций, по которым не были составлены сообщения, службами внутреннего аудита, внутреннего

контроля криптобанка, Секретариатом Наблюдательного совета Парка высоких технологий, Национальным банком и иными государственными органами, осуществляющими контроль за соблюдением банками законодательства в сфере ПОД/ФТ. Система считается адекватной, если количество ненаправленных специальных формуляров не превышает 5 процентов от общего количества направленных специальных формуляров.

36. Для установления адекватной системы критериев выявления и признаков подозрительных финансовых операций криптобанк классифицирует клиентов, с которыми заключены договоры на осуществление финансовых операций в письменной форме, по следующим категориям:

крупные;

средние;

малые.

Криптобанк вправе классифицировать по категориям, указанным в части первой настоящего пункта, клиентов, осуществляющих разовые операции.

Криптобанк самостоятельно определяет в правилах внутреннего контроля банка порядок отнесения клиента к категории крупных, средних или малых.

Присвоенная криптобанком категория клиента указывается в разделе ”Служебная информация“ анкеты клиента.

37. Анализ показателей адекватности системы критериев выявления и признаков подозрительных финансовых операций проводится криптобанком по мере необходимости, но не реже одного раза в течение календарного года. Если показатели адекватности выходят за пределы установленных границ, криптобанком пересматривается хотя бы одно из значений:

анализируемого периода по видам финансовых операций;

корректировок критериев выявления и признаков подозрительных финансовых операций;

критериев отнесения клиентов к категориям;

итоговой степени риска работы с отдельными клиентами.

При определении в правилах внутреннего контроля суммы финансовой операции, близкой по значению к установленным в критериях выявления и признаках подозрительных финансовых операций пороговым величинам, используются границы отклонения не менее 5 процентов. В зависимости от вида финансовых операций предельное значение отклонения может составлять до 10 процентов.

38. В целях мониторинга рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, криптобанк проводит самооценку вовлеченности в проведение

подозрительных операций, связанных с получением и (или) легализацией доходов, полученных преступным путем, финансированием террористической деятельности, распространением или финансированием распространения оружия массового поражения, с использованием следующих показателей:

38.1. коэффициент (в процентах) вовлеченности криптобанка в проведение подозрительных финансовых операций его клиентами при осуществлении банковских операций, определяемый как отношение суммы подозрительных финансовых операций, осуществленных клиентами криптобанка и установленных в соответствии с Рекомендациями по критериям выявления и признакам подозрительных финансовых операций, связанных с получением и (или) легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения при осуществлении банковских операций, утвержденными постановлением Правления Национального банка Республики Беларусь от 29 марта 2023 г. № 113 (далее – Рекомендации 113), к сумме дебетовых оборотов по счетам клиентов криптобанка;

38.2. коэффициент (в процентах) вовлеченности криптобанка в проведение подозрительных финансовых операций его клиентами при осуществлении операций с цифровыми знаками (токенами), определяемый как отношение суммы подозрительных финансовых операций, осуществленных клиентами криптобанка и установленных в соответствии с критериями, установленными приложением 5 к Положению о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий, утвержденному решением Наблюдательного совета Парка высоких технологий (протокол от 23 октября 2018 г. № 08/НС-5пр), к сумме ввода средств на криптоаккаунты клиентов криптобанка;

38.3. величина (в процентах) удельного веса подозрительных финансовых операций по признакам подозрительности, определяемая как отношение суммы подозрительных финансовых операций, осуществленных клиентами криптобанка, приходящейся на цифровой код признаков подозрительности финансовых операций в соответствии со справочником признаков подозрительности финансовых операций, установленным приложением 4 к Инструкции о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю, к общей сумме подозрительных финансовых операций, осуществленных клиентами криптобанка;

38.4. критерий реализации криптобанком права на отказ в осуществлении подозрительных финансовых операций, оцениваемый при одновременном сопоставлении двух показателей:

величина (в процентах) удельного веса специальных формуляров с правом на отказ, определяемая как количество специальных формуляров, направленных по операциям, соответствующим признакам, которые согласно правилам внутреннего контроля могут являться основаниями для отказа в осуществлении финансовой операции (за исключением поступления денежных средств), отказа в подключении к системе дистанционного обслуживания, прекращения или приостановления оказания услуг посредством этой системы, в общем количестве направленных специальных формуляров;

коэффициент (в процентах) реализации права на отказ в осуществлении подозрительных финансовых операций, определяемый как отношение количества специальных формуляров, содержащих информацию об отказе в осуществлении финансовой операции, об отказе в подключении к системе дистанционного обслуживания, о прекращении или приостановлении оказания услуг посредством этой системы, об отказе от исполнения договора на осуществление финансовых операций в письменной форме или отказе в заключении такого договора, к количеству специальных формуляров, направленных по финансовым операциям, соответствующим признакам, которые согласно правилам внутреннего контроля могут являться основаниями для отказа в осуществлении финансовой операции (за исключением поступления денежных средств), отказа в подключении к системе дистанционного обслуживания, прекращения или приостановления оказания услуг посредством этой системы;

38.5. величина (в процентах) удельного веса клиентов с высокой степенью риска в клиентской базе, определяемая как отношение количества клиентов, работе с которыми криптобанком присвоена высокая итоговая степень риска, к общему количеству клиентов (всего и по группам клиентов криптобанка (физические лица, индивидуальные предприниматели, организации, банки-респонденты, криптобанки-респонденты);

38.6. величина (в процентах) удельного веса клиентов, в отношении которых представлялись специальные формуляры, к количеству клиентов, которые проводили финансовые операции по счетам на основании платежных инструкций за анализируемый период (всего и по группам клиентов);

38.7. величина (в процентах) удельного веса клиентов, в отношении которых представлялись специальные формуляры, к количеству клиентов, которые проводили финансовые операции с использованием цифровых знаков (токенов) на основании заявок на вывод цифровых знаков (токенов) с криптоаккаунтов за анализируемый период (всего и по группам клиентов);

38.8. величина (в процентах) удельного веса клиентов, в отношении которых представлялись специальные формуляры, к количеству клиентов, которые проводили финансовые операции по криптоаккаунтам с использованием цифровых знаков (токенов) за анализируемый период (всего и по группам клиентов);

38.9. иные показатели, определяемые криптобанком.

39. Расчет коэффициента вовлеченности криптобанка в проведение подозрительных финансовых операций его клиентами осуществляется криптобанком ежемесячно. Расчет остальных показателей самооценки вовлеченности криптобанка в проведение подозрительных операций, связанных с получением и (или) легализацией доходов, полученных преступным путем, финансированием террористической деятельности, распространением или финансированием распространения оружия массового поражения, проводится с периодичностью, позволяющей обеспечить своевременное принятие управленческих решений, направленных на совершенствование системы внутреннего контроля.

Криптобанки самостоятельно определяют показатели из числа показателей, установленных в пункте 38 настоящего Положения, в соответствии с характером и объемом осуществляемых операций.

40. В целях ограничения (снижения) рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, криптобанк применяет следующие расширенные меры внутреннего контроля:

40.1. в отношении всех клиентов:

отказ в осуществлении финансовой операции в случае непредставления клиентом сведений и документов, необходимых для проведения идентификации, а также обновлении (актуализации) данных о клиенте;

запрос при необходимости сведений и документов (их копий) для пояснения сути проводимых финансовых операций;

анализ финансовых операций на их соответствие сведениям криптобанка о клиенте, цели и характеру его деятельности, в том числе по определению источника происхождения денежных средств клиента для оперативного выявления подозрительных финансовых операций, и его документирование;

иные меры, состав которых определяется криптобанком самостоятельно в соответствии с законодательством;

40.2. в отношении банков-респондентов и криптобанков-респодентов:

осуществление оценки достаточности мер, принимаемых банком-респондентом, криптобанком-респондентом в целях ПОД/ФТ при установлении корреспондентских отношений, документирование

результатов проведенной оценки, ее обновление (актуализация) по мере необходимости;

выявление использования корреспондентского счета другими иностранными банками (банки-респонденты, криптобанки-респонденты второго уровня);

определение ответственности каждой из сторон (банка-респондента и банка-корреспондента, криптобанка-респондента и криптобанка-корреспондента) и возможности получения информации о надлежащей проверке клиента иностранного банка-респондента, криптобанка-респондента, клиентов банков-респондентов и криптобанков-респондентов второго уровня по запросу банка, криптобанка;

иные меры, состав которых определяется криптобанком самостоятельно в соответствии с законодательством;

40.3. в отношении клиентов-резидентов из числа лиц, осуществляющих финансовые операции, и в отношении клиентов-нерезидентов (за исключением банков-респондентов, криптобанков-респондентов) из числа финансовых учреждений и нефинансовых организаций, определенных в рекомендациях Группы разработки финансовых мер борьбы с отмыванием денег:

осуществление оценки достаточности мер, принимаемых клиентом в целях ПОД/ФТ, документирование результатов проведенной оценки, ее обновление (актуализация) по мере необходимости;

установление наименования и места нахождения надзорного органа страны нахождения клиента-нерезидента, периодичности проводимых им проверок;

проведение личных встреч для выяснения качества организации системы внутреннего контроля клиента в сфере ПОД/ФТ;

иные меры, состав которых определяется криптобанком самостоятельно в соответствии с законодательством;

40.4. в отношении своих контрагентов по финансовым операциям:

осуществление оценки риска контрагента-нерезидента, включая банк-корреспондент и криптобанк-корреспондент, как вероятности вовлечения криптобанка в финансовые операции, связанные с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, документирование результатов проведенной оценки, ее обновление (актуализация) по мере необходимости;

установление бенефициарного владельца;

регистрация финансовых операций, подлежащих особому контролю, включая финансовые операции по привлечению криптобанком займов от нерезидентов, в специальном формуляре и представление его в виде электронного документа в орган финансового мониторинга;

иные меры, состав которых определяется криптобанком самостоятельно в соответствии с законодательством;

40.5. в отношении клиентов, работе с которыми установлена высокая итоговая степень риска:

усиленный мониторинг финансовых операций клиента (осуществление финансовых операций после получения и оценки документов, подтверждающих финансовую операцию клиента, и их согласования с подразделением комплаенс-контроля);

отказ клиенту в осуществлении финансовой операции (за исключением поступления денежных средств), если финансовая операция отвечает критериям выявления и признакам подозрительных финансовых операций, которые могут являться согласно правилам внутреннего контроля основанием для отказа в ее осуществлении;

приостановление финансовой операции (за исключением поступления денежных средств), но не более чем на два рабочих дня, включая день, когда распоряжение клиента о ее осуществлении должно быть выполнено, для принятия решения об осуществлении финансовой операции либо отказе в ее осуществлении в соответствии с абзацем третьим настоящего подпункта;

отказ клиенту в осуществлении финансовой операции, если имеется информация о причастности банка, криптобанка, в том числе банка-нерезидента и криптобанка-нерезидента, в котором открыт счет получателя денежных средств, либо получателя денежных средств к незаконным финансовым операциям или применении к ним санкций;

отказ клиенту в одностороннем порядке от исполнения договора на осуществление финансовых операций в письменной форме при наличии в течение шести месяцев двух и более решений об отказе в осуществлении финансовых операций клиента с обязательным его письменным уведомлением

отказ клиенту в подключении к системе дистанционного обслуживания, прекращение или приостановление оказания услуг посредством этой системы, если осуществляемые им финансовые операции отвечают критериям отказа в подключении (прекращения, приостановления), которые могут являться согласно правилам внутреннего контроля основанием для таких действий;

верификация. Верификация может применяться в отношении клиентов, которым присвоена высокая степень риска хотя бы по одному из векторов трехвекторной модели распределения рисков;

установление ограничений по предоставлению услуг (продуктов) и способам их оказания;

иные меры, состав которых определяется криптобанком самостоятельно в соответствии с законодательством;

40.6. в отношении клиентов-нерезидентов, идентификация которых осуществлена на удаленной основе:

отказ клиенту в финансовой операции, связанной с зачислением на криптокарточку либо счет клиента денежных средств, поступивших посредством перевода с банковской платежной карточки, эмитированной банком Республики Беларусь, либо со счета физического лица-резидента;

запрет на пополнение текущего (расчетного) счета или иного счета клиента, в том числе доступ к которому обеспечивается посредством использования криптокарточки, наличными денежными средствами;

40.7. в отношении услуг (продуктов) криптобанка, которым установлена высокая присущая степень риска:

определяются методы (инструменты) ограничения (снижения) рисков;

формируется система лимитов и (или) ограничений (лимитная политика) в отношении отдельных клиентов, групп клиентов, финансовых операций и их видов, направлений деятельности, а также порядок контроля применения и соблюдения лимитной политики, принятия надлежащих мер руководством криптобанка.

41. Решение о применении расширенных мер внутреннего контроля, указанных в подпунктах 40.1 - 40.5 и 40.7 пункта 40 настоящего Положения, принимается криптобанком самостоятельно.

Расширенные меры внутреннего контроля, предусмотренные подпунктом 40.6 пункта 40 настоящего Положения, являются обязательными для применения криптобанком.

Обстоятельства, при которых применяются расширенные меры внутреннего контроля, указанные в части первой настоящего пункта, определяются в правилах внутреннего контроля.

Решение о применении расширенных мер внутреннего контроля принимает ответственное должностное лицо криптобанка.

Целью принимаемых расширенных мер внутреннего контроля должна являться минимизация риска возможного вовлечения как криптобанка, так и его работников в процессы легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения.

ГЛАВА 4
ИДЕНТИФИКАЦИЯ И АНКЕТИРОВАНИЕ КЛИЕНТОВ. ВЕРИФИКАЦИЯ

42. Криптобанк до приема на обслуживание идентифицирует клиента в соответствии со статьей 8 Закона №165-З.

Криптобанк вправе осуществлять идентификацию на удаленной основе в порядке, установленном Советом Министров Республики Беларусь и Национальным банком Республики Беларусь.

43. В случае если криптобанк в соответствии с частью двадцать пятой статьи 8 Закона № 165-З поручил проведение идентификации клиента агенту по идентификации, такой криптобанк определяет в правилах внутреннего контроля порядок взаимодействия с агентами по идентификации.

Криптобанк, поручивший проведение идентификации, несет ответственность за соблюдение требований по идентификации, установленных Законом № 165-З и иными актами законодательства.

44. Криптобанк устанавливает идентификационные данные на основании сведений и документов (их копий, или изображений, созданных путем сканирования, или фотографических изображений, или видеоизображений (далее - изображения)), в том числе документов, являющихся основанием для осуществления банковских операций, операций с цифровыми знаками (токенами), которые предоставлены клиентом либо агентом по идентификации, получены криптобанком из систем идентификации или от регистрирующего органа, а также из иных не запрещенных законодательством источников.

С целью проведения идентификации клиенту предоставляется для заполнения вопросник (при личном присутствии клиента в процессе общения с работником криптобанка, агента по идентификации) либо электронная регистрационная карта (размещенная на сайте криптобанка в глобальной компьютерной сети Интернет или предложенная клиенту для заполнения на основе программно-информационных сервисов или иным образом).

45. Правила внутреннего контроля должны содержать сведения о применяемых криптобанком системах идентификации (включая сведения о порядке их использования).

Использование криптобанком систем идентификации, не соответствующих рекомендациям ФАТФ, не допускается.

46. Криптобанк фиксирует данные, установленные в ходе проведения идентификации клиентов, в электронной базе данных анкет клиентов (далее – электронная база данных анкет клиентов) при:

заключении договоров на осуществление финансовых операций в письменной форме;

осуществлении финансовых операций с денежными средствами (электронными деньгами), сумма которых равна или превышает 1000 базовых величин, клиентами, осуществляющими разовые операции;

осуществлении операций с цифровыми знаками (токенами), сумма которых равна или превышает 1000 долларов США в эквиваленте, клиентами, осуществляющими разовые операции;

осуществлении финансовых операций, подлежащих особому контролю, независимо от того, были они осуществлены или нет, при наличии идентификационных данных клиента.

Внесение идентификационных данных в электронную базу данных анкет клиентов осуществляется посредством заполнения анкеты клиента. В случае необходимости после проведения верификации данные, внесенные в анкету клиента, корректируются криптобанком.

Идентификационные данные о представителе клиента фиксируются в анкете клиента.

Идентификационные данные о контрагенте криптобанка по финансовым операциям могут фиксироваться в электронной базе данных анкет клиентов криптобанка.

Если бенефициарными владельцами клиента являются несколько физических лиц, каждый из которых владеет не менее чем 10 процентами акций (долей в уставном фонде, паев), то в анкету клиента вносятся идентификационные данные о каждом бенефициарном владельце.

При анкетировании граждан Республики Беларусь, иностранных граждан и лиц без гражданства, имеющих вид на жительство в Республике Беларусь, в качестве реквизитов документа, удостоверяющего личность, используется идентификационный номер.

Для каждой группы клиентов (физические лица, индивидуальные предприниматели, организации (за исключением банков-респондентов, криптобанков-респондентов), банки-респонденты, криптобанки-респонденты) криптобанком разрабатывается анкета клиента, которая является внутренним документом криптобанка.

Анкета клиента заполняется в электронном виде. Криптобанк обеспечивает ведение электронной базы данных анкет клиентов.

При поручении проведения идентификации агенту по идентификации допускается ведение электронной базы данных анкет клиентов криптобанка агентом по идентификации. При этом агент по идентификации обеспечивает криптобанку оперативный доступ к электронной базе данных анкет клиентов криптобанка.

47. Форма анкеты клиента разрабатывается с учетом особенностей деятельности криптобанка и осуществляемых финансовых операций, а также требований статьи 8 Закона № 165-З.

В зависимости от присвоенной работе с клиентом степени риска анкета может быть стандартной или расширенной формы.

Анкета клиента стандартной формы содержит перечень идентификационных данных, фиксируемых в соответствии со статьей 8 Закона № 165-З, цели установления и предполагаемый характер отношений с криптобанком и аналитический раздел ”Служебная информация“.

Анкета клиента расширенной формы также содержит перечень дополнительных идентификационных данных согласно приложению 4. Дополнительные идентификационные данные запрашиваются криптобанком у клиента либо получаются им из иных не запрещенных законодательством источников. В случае отказа клиента от предоставления дополнительных идентификационных данных криптобанк обязан отказать клиенту в осуществлении финансовой операции.

По решению криптобанка анкета клиента может дополняться иными данными, которые криптобанк считает необходимыми для применения расширенных мер по идентификации клиентов.

При определении объема идентификационных сведений третьих лиц (кроме банков-корреспондентов), указываемых в анкете клиента, криптобанк руководствуется перечнем обязательных сведений, установленным для анкеты стандартной формы, с учетом объема идентификационных данных, которыми располагает клиент в отношении третьего лица и которые третье лицо идентифицируют.

48. В аналитическом разделе ”Служебная информация“ анкеты клиента указываются:

48.1. присвоенная степень риска работы с клиентом (итоговая и по каждому вектору модели);

48.2. обоснование высокой итоговой степени риска и (или) по векторам модели;

48.3. решение ответственного должностного лица о способе верификации и сроки ее выполнения;

48.4. решение ответственного должностного лица о дальнейших действиях в отношении клиента, предусмотренных частью второй пункта 87 настоящего Положения;

48.5. основание для признания в качестве бенефициарного владельца клиента, который является организацией, лица, осуществляющего функции единоличного исполнительного органа, либо лица, возглавляющего коллегиальный исполнительный орган (при невозможности достоверного установления бенефициарного владельца);

48.6. причины возникновения подозрений, предусмотренных в пункте 59 настоящего Положения;

48.7. решение ответственного должностного лица криптобанка о принятии дальнейших расширенных мер в отношении клиента, направленных на ограничение (снижение) рисков, предусмотренных пунктом 40 настоящего Положения, и сроки их выполнения;

48.8. решение ответственного должностного лица о замораживании средств и (или) блокировании финансовой операции в отношении лиц, причастных к террористической деятельности;

48.9. решение ответственного должностного лица о приостановлении финансовой операции или отказе в ее осуществлении, об отказе в

одностороннем порядке от исполнения договора на осуществление финансовых операций в письменной форме, отказе в подключении клиента к системе дистанционного обслуживания, о прекращении или приостановлении оказания услуг посредством этой системы;

48.10. даты заполнения и обновления (актуализации) анкеты клиента;

48.11. причины отсутствия идентификационных данных и меры, принятые криптобанком для их получения;

48.12. сведения о финансовых операциях с денежными средствами (электронными деньгами), сумма которых равна или превышает 1000 базовых величин, с цифровыми знаками (токенами), сумма которых равна или превышает 1000 долларов США в эквиваленте, клиентов, осуществляющих разовые операции:

дата и место осуществления финансовой операции;

сумма финансовой операции;

вид финансовой операции в соответствии с приложением 2 к Инструкции о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю.

Для финансовых операций, подлежащих особому контролю, указываются:

номер и дата представления специального формуляра в орган финансового мониторинга;

код признака подозрительности финансовой операции в соответствии с приложением 4 к Инструкции о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю;

48.13. категория клиента, присвоенная согласно части первой пункта 36 настоящего Положения;

48.14. сведения, необходимые для понимания цели и характера деятельности клиента, документы криптобанка (ссылки либо гиперссылки на документы), составленные и (или) полученные либо имеющиеся в распоряжении криптобанка в ходе принятия мер, направленных на ограничение (снижение) рисков, предусмотренных пунктом 40 настоящей Инструкции, и результат анализа указанных сведений и документов.

48.15. иные сведения, необходимые для формирования представлений о клиенте.

49. Анкета расширенной формы заполняется:

по клиентам, работа с которыми оценивается криптобанком высокой итоговой степенью риска;

по банкам-респондентам, криптобанкам-респондентам;

по клиентам-резидентам, относящимся к лицам, осуществляющим финансовые операции, и клиентам-нерезидентам, относящимся к

финансовым и нефинансовым организациям, определенным в общем словаре терминов Международных стандартов по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (Рекомендации ФАТФ);

по клиентам, зарегистрированным, имеющим место жительства или место нахождения в государстве (на территории), которое (которая) не участвует в международном сотрудничестве в сфере ПОД/ФТ либо не выполняет Рекомендации ФАТФ, а также если их финансовые операции осуществляются с использованием счета в банке, зарегистрированном в таком государстве (на территории);

по решению ответственного должностного лица;

по иным основаниям, предусмотренным правилами внутреннего контроля.

50. Криптобанк обеспечивает:

оперативный доступ к электронной базе данных анкет клиентов либо к ее части ответственным должностным лицам, а также работникам криптобанка, осуществляющим обслуживание клиентов;

проверку программным путем сведений о клиентах и их бенефициарных владельцах с целью отнесения их к публичным должностным лицам (дата проверки, наличие (отсутствие) совпадений, сведения о клиенте при наличии совпадения);

по мере внесения изменений в перечень в соответствии с установленным законодательством, но не реже одного раза в три месяца, проверку программным путем сведений о клиентах и их бенефициарных владельцах с целью выявления лиц, включенных в перечень, с отражением результатов истории проверок (дата проверки, наличие (отсутствие) совпадений, сведения о клиенте (его представителе, выгодоприобретателе) в случае совпадения) в журнале учета проверок, форму которого криптобанк устанавливает самостоятельно. Ведение журнала осуществляется в электронном виде.

51. Криптобанки обеспечивают сохранность и целостность информации о клиентах, содержащейся в электронной базе данных анкет клиентов, в том числе при сбоях (отказах) технических и программных средств.

Распространение и (или) предоставление информации, содержащейся в электронной базе данных анкет клиентов, осуществляется криптобанком с соблюдением требований законодательства об информации, информатизации и защите информации.

52. Срок хранения анкеты клиента криптобанка соответствует сроку, указанному в абзаце четырнадцатом части первой статьи 6 Закона № 165-З для хранения сведений и документов (их копий, изображений), полученных в результате идентификации клиентов.

53. Электронная база данных анкет клиентов криптобанка должна обеспечивать:

ведение истории анкет клиентов с возможностью просмотра изменений, в том числе на основании верификации, и дат их внесения по каждому клиенту;

ведение истории обновления (актуализации) анкеты клиента (когда и кем анкета клиента была обновлена (актуализирована));

ведение журнала (реестра) изменений (когда, кем и какие были внесены изменения в анкеты клиентов);

наличие поисковых систем, позволяющих делать выборку (фильтр) анкет клиентов, удовлетворяющих заданным параметрам. При этом поиск осуществляется по любым из идентификационных данных клиентов;

отображение информационных связей между клиентами, в том числе организацией и физическим лицом, являющимся руководителем, учредителем или бенефициарным владельцем этой организации, а также поиск связанных друг с другом клиентов;

печать анкет клиентов, включая раздел ”Служебная информация“.

54. При заполнении анкет клиентов в электронной базе данных анкет клиентов при отсутствии у клиента данных (характеристик, параметров) соответствующая графа может не заполняться, в ней допускается ставить прочерк или указывать слова ”нет“, ”отсутствует“, ”не имеет“.

55. Анкетирование новых клиентов, которым открывается текущий (расчетный) банковский счет, криптоаккаунт, осуществляется до открытия этого счета, криптоаккаунта на основании документов, представляемых в соответствии с законодательством. В течение месяца после открытия клиенту текущего (расчетного) банковского счета, криптоаккаунта криптобанк дополняет его анкету данными, которые отсутствовали на момент открытия этого счета. В договоре между криптобанком и клиентом могут быть определены порядок и условия представления клиентом сведений и документов (их копий), необходимых криптобанку для выполнения возложенных на него законодательством обязанностей по ПОД/ФТ.

56. Криптобанки при проведении идентификации участников финансовой операции и осуществлении финансовых операций, связанных с внутренними банковскими, денежными переводами по поручению отправителя (плательщика), руководствуются требованиями пунктов 58 и 58-1 Инструкции № 818.

57. Криптобанки при проведении идентификации участников финансовой операции и осуществлении финансовых операций, связанных с банковскими, денежными переводами по поручению отправителя (плательщика) (кроме финансовых операций с использованием банковских платежных карточек, платежей, осуществляемых посредством единого расчетного и информационного пространства, расчетов

посредством прямого дебетования счета), должны обеспечить на любом этапе их осуществления установление, передачу и хранение в соответствии с абзацем четырнадцатым части первой статьи 6 Закона № 165-З данных, предусмотренных частями двадцатой и двадцать первой статьи 8 Закона № 165-З.

58. Криптобанки обновляют (актуализируют) данные:

по клиентам, работе с которыми присвоена высокая итоговая степень риска, – не реже одного раза в течение календарного года;

по клиентам, работе с которыми присвоена средняя итоговая степень риска, – не реже одного раза в течение двух календарных лет;

по клиентам, работе с которыми присвоена низкая итоговая степень риска, – не реже одного раза в течение трех календарных лет.

Криптобанки обновляют (актуализируют) данные о клиенте в порядке (способом), установленном в договоре, заключаемом с клиентом.

59. При наличии подозрений в достоверности и (или) точности полученных ранее данных криптобанки обновляют данные, полученные в результате идентификации в течение двадцати рабочих дней, следующих за днем принятия решения ответственным должностным лицом криптобанка о наличии таких подозрений.

60. Криптобанк вправе предоставить клиентам, являющимся индивидуальными предпринимателями, организациями и физическими лицами, представленные ими ранее идентификационные данные для их подтверждения и использования в целях обновления (актуализации) данных анкет клиентов.

Криптобанки обязаны предусматривать в заключаемых с клиентами договорах в качестве существенного условия обязанность клиентов уведомлять криптобанки об изменении идентификационных данных, предусмотренных статьей 8 Закона № 165-З, в срок не более трех дней с даты возникновения соответствующих изменений.

61. Идентификационные данные о клиентах, осуществляющих разовые операции, обновляются (актуализируются) при осуществлении ими следующих финансовых операций:

финансовой операции с денежными средствами (электронными деньгами), сумма которой равна или превышает 1000 базовых величин;

операции с цифровыми знаками (токенами), сумма которых равна или превышает 1000 долларов США в эквиваленте;

финансовой операции, подлежащей особому контролю.

62. Обновление (актуализация) идентификационных данных о клиентах, осуществивших идентификацию на удаленной основе, осуществляется в порядке, установленном Советом Министров Республики Беларусь и Национальным банком Республики Беларусь для проведения идентификации клиентов на удаленной основе.

63. В электронную базу данных анкет клиентов криптобанк вносит:

идентификационные данные нового клиента – в течение 3 рабочих дней после заключения с ним договора на осуществление финансовых операций в письменной форме;

идентификационные данные, отличные от данных, указанных в анкете клиента, – в течение 3 рабочих дней после их предоставления клиентом и (или) получения криптобанком;

идентификационные данные клиента, переданные криптобанку агентом по идентификации, – в течение 3 рабочих дней после их получения криптобанком от агента по идентификации;

идентификационные данные нового клиента, осуществляющего разовые операции, – в течение 3 рабочих дней после осуществления финансовой операции, сумма которой равна или превышает 1000 базовых величин, либо финансовой операции, подлежащей особому контролю;

идентификационные данные нового клиента, осуществляющего разовые операции, – в течение 3 рабочих дней после осуществления операции с цифровыми знаками (токенами), сумма которой равна или превышает 1000 базовых величин, либо финансовой операции, подлежащей особому контролю;

сведения о подозрительной финансовой операции клиента – в течение 3 рабочих дней после направления специального формуляра в орган финансового мониторинга;

идентификационные данные клиента, подлежащие обновлению (актуализации) в соответствии с пунктом 61 настоящего Положения, – в течение 7 рабочих дней после их предоставления клиентом и (или) получения криптобанком;

решения ответственного должностного лица о дальнейших действиях криптобанка в отношении клиента – в день принятия такого решения ответственным должностным лицом.

64. Обновление (актуализация) содержащихся в анкетах клиентов данных не является обязательным в случае, когда клиентом криптобанка не проводятся операции в течение 6 месяцев, предшествующих дате истечения установленного срока обновления (актуализации) анкеты, при невозможности установления контакта с данными клиентами, либо в случае, когда клиентом не проводятся операции в течение срока, установленного для обновления (актуализации) анкет клиентов.

65. Криптобанк при верификации сверяет полученные из различных источников информации идентификационные данные и при необходимости уточняет и дополняет данные, полученные в ходе идентификации клиента. Для верификации криптобанк вправе:

запрашивать и получать в порядке и пределах, установленных законодательством, информацию о клиенте в государственных органах и иных организациях;

использовать для проверки и дополнения данных, полученных в ходе идентификации, открытые источники информации, базы данных;

осуществлять сверку идентификационных данных, полученных из систем идентификации, с данными, содержащимися в документе, удостоверяющим личность, в учредительных, регистрационных и (или) иных документах;

осуществлять сверку представленных идентификационных данных индивидуального предпринимателя, организации с данными, присвоенными государственными органами;

контактировать с клиентом, его представителем при личной встрече, по телефону, письменно, посредством электронной почты, с использованием иных каналов связи для дистанционной передачи данных;

установить в правилах внутреннего контроля иные не противоречащие законодательству мероприятия по верификации.

66. Для осуществления верификации криптобанк принимает следующие меры (одну или несколько данных мер в зависимости от сложившихся обстоятельств с учетом части второй настоящего пункта):

осуществляет сверку представленных клиентом идентификационных данных с данными о нем, полученными из общедоступных и других источников в соответствии с законодательством, в том числе в социальных сетях;

контактирует с клиентом, его представителем при личной встрече, по телефону, письменно, посредством электронной почты или установления видеосвязи с клиентом в глобальной компьютерной сети Интернет;

отслеживает адрес интернет-протокола клиента;

осуществляет изучение общедоступных источников информации (в том числе в глобальной компьютерной сети Интернет) на предмет наличия в отношении клиентов и (или) их бенефициарных владельцев компрометирующей информации;

осуществляет поиск в глобальной компьютерной сети Интернет информации, подтверждающей, что деятельность, которую осуществляет клиент, совместима (не совместима) с финансовыми операциями, участником которых он является либо планирует выступить;

применяет процедуру web-ID, которая осуществляется на удаленной основе посредством установления видеосвязи с клиентом в глобальной компьютерной сети Интернет, для подтверждения достоверности ранее представленных клиентом идентификационных данных;

получает от клиента направленные клиентом с адреса электронной почты, указанного в электронной регистрационной карте (вопроснике), на адрес электронной почты криптобанка либо иным образом, определенным криптобанком, изображения надлежащего качества следующих документов (материалов):

для физического лица – фотоизображение, на котором изображен клиент с документом, удостоверяющим его личность, открытым на страницах, содержащих личные данные и фотографию (вместо данного изображения может быть представлено видеоизображение надлежащего качества, в котором заснят клиент с документом, удостоверяющим его личность, открытым на страницах, содержащих личные данные и фотографию);

для организации – фотоизображение, на котором изображен представитель клиента - организации с документом, удостоверяющим его личность, открытым на страницах, содержащих личные данные и фотографию, и документом, подтверждающим полномочия этого представителя (вместо указанных фотоизображения и документа может быть представлено видеоизображение надлежащего качества, в котором заснят представитель клиента - организации с указанными документами);

использует технологию Liveness check (программное обеспечение, позволяющее определить лицо живого человека по нескольким параметрам);

проводит сравнение биометрических моделей, сформированных на основании изображения лица клиента – физического лица или лица представителя клиента – организации и их фотографии из документа, удостоверяющего личность, и определяет степень их сходства;

использует для проверки и дополнения данных, полученных в ходе идентификации, открытые источники информации, базы данных;

знакомится с аудиторским заключением, подготовленным по итогам проведения обязательного аудита годовой бухгалтерской (финансовой) отчетности клиента;

получает от клиента документы (их копии, изображения), необходимые криптобанку для проведения верификации, определенные криптобанком;

получает данные о клиенте из систем идентификации;

устанавливает в правилах внутреннего контроля и применяет иные не противоречащие законодательству способы верификации.

По итогам проведения верификации у криптобанка должно сформироваться разумное убеждение о том, что его клиент является именно тем лицом, которым клиент представился.

При получении от клиента изображений документов (материалов), указанных в абзацах восьмом – десятом части первой настоящего пункта, обязательным является одновременное получение перевода этих документов (материалов) на английский или русский (белорусский) язык, если данные документы (материалы) выполнены (составлены) на ином языке и указанный перевод не был предоставлен (осуществлен) при идентификации. Осуществление (обеспечение осуществления) такого перевода вправе принять на себя криптобанк.

67. В правилах внутреннего контроля должна быть предусмотрена зависимость выбора способов верификации, предусмотренных в пункте 66 настоящего Положения, от сложившихся обстоятельств и итоговой степени риска работы с клиентом, учтена необходимость обеспечения эффективности процедуры верификации, определены сроки проведения верификации, если они не установлены пунктом 68 настоящего Положения.

68. Проведение дополнительной верификации с использованием одного из способов, предусмотренных абзацами седьмым – десятым и одиннадцатым части первой пункта 66 настоящего Положения, осуществляется в соответствии с требованиями пункта 52 Положения о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий.

69. Сведения и документы (их копии, изображения), полученные (созданные) криптобанком в ходе идентификации клиентов, их представителей, иные сведения, полученные криптобанком в ходе верификации в отношении клиента, могут помещаться в досье клиента, которое может вестись на бумажном носителе и (или) в электронном виде.

70. Идентификационные данные клиентов, сведения об источниках происхождения средств клиентов, должны храниться криптобанками на бумажном носителе и (или) в электронном виде в месте, исключающем доступ посторонних лиц, в течение 5 лет с даты прекращения действия заключенных с ними криптобанками договоров.

Криптобанки обязаны принимать меры по обеспечению сохранности сведений (информации), в том числе посредством осуществления резервного копирования), а также по соблюдению требований по защите персональных данных, предусмотренных законодательством Республики Беларусь.

ГЛАВА 5
ЗАМОРАЖИВАНИЕ СРЕДСТВ И (ИЛИ) БЛОКИРОВАНИЕ ФИНАНСОВЫХ ОПЕРАЦИЙ

71. Криптобанки замораживают средства и (или) блокируют финансовую операцию в случаях, определенных частью первой статьи 9^1 Закона № 165-З.

Принятие мер по замораживанию средств и (или) блокированию финансовой операции должно обеспечить невозможность использования средств лицами, включенными в перечень, либо организациями, бенефициарными владельцами которых являются физические лица, включенные в перечень.

Криптобанк информирует клиента о запрете на распоряжение, пользование средствами в связи с его включением в перечень либо включением в перечень физического лица, являющегося бенефициарным

владельцем организации, порядке получения разрешения органа финансового мониторинга на осуществление финансовых операций для обеспечения жизнедеятельности физического лица, в том числе индивидуального предпринимателя, и порядке обжалования решения о включении в перечень после получения письменного обращения клиента.

Криптобанк информирует клиента о запрете на осуществление финансовой операции в связи с включением участника финансовой операции, выгодоприобретателя по финансовой операции либо физического лица, являющегося бенефициарным владельцем организации, в перечень при блокировании финансовой операции или после получения письменного обращения клиента.

Криптобанк информирует орган финансового мониторинга о замораживании средств и (или) блокировании финансовой операции путем направления специального формуляра.

72. Криптобанк использует программное обеспечение и (или) иные технологические средства, позволяющие автоматически выявлять клиентов, средства которых подлежат замораживанию, и обнаруживать финансовую операцию, подлежащую блокированию, до ее проведения.

73. Криптобанки определяют в правилах внутреннего контроля:

порядок получения и обновления на постоянной основе в информационной системе криптобанка перечня (с официального сайта уполномоченного государственного органа в глобальной компьютерной сети Интернет или его мессенджера, либо посредством автоматизированной системы поиска информации, содержащей сведения из этого перечня);

лиц, ответственных за получение и обновление перечня;

лицо, уполномоченное (лиц, уполномоченных) выявлять среди клиентов криптобанка организаций, индивидуальных предпринимателей и физических лиц, в отношении которых должны быть применены меры по замораживанию средств и (или) блокированию финансовых операций;

форму и способ уведомления клиента о замораживании средств и (или) блокировании финансовой операции, а также о размораживании средств и (или) разблокировании финансовой операции;

порядок учета (хранения) средств, в отношении которых применены меры по замораживанию средств и (или) блокированию финансовых операций;

порядок размораживания средств и (или) разблокирования финансовых операций при наличии у криптобанка информации об исключении организации, индивидуального предпринимателя, физического лица из перечня либо при наличии соответствующего извещения органа финансового мониторинга об отмене решения о замораживании средств и (или) блокировании финансовой операции в

случае установления по результатам проверки непричастности клиента к террористической деятельности;

порядок осуществления финансовых операций для обеспечения жизнедеятельности физических лиц, в том числе индивидуальных предпринимателей, денежные средства которых заморожены, по разрешению органа финансового мониторинга.

74. Криптобанки применяют меры по замораживанию средств клиентов, хранящихся на банковских счетах, криптоаккаунтах, криптовкладах, цифровых знаков (токенов), находящихся на кастодиальном хранении, а также иных средств незамедлительно, но не позднее одного рабочего дня со дня получения в установленном порядке перечня либо внесения изменений в перечень. Криптобанк после включения клиента в перечень продолжает перечислять на счета этого клиента проценты по вкладу (депозиту), криптовкладу, иным банковским счетам и криптоаккаунтам клиента, если уплата таких процентов предусмотрена договором.

Средства, поступившие клиентам криптобанка, в отношении которых применены меры по замораживанию, также подлежат замораживанию.

Криптобанки не реже одного раза в три месяца проверяют наличие среди своих клиентов лиц, в отношении которых должны быть применены меры по замораживанию средств, и при выявлении таких клиентов незамедлительно, но не позднее одного рабочего дня со дня выявления замораживают эти средства.

75. При идентификации нового клиента криптобанк осуществляет проверку нахождения такого клиента, его представителей, выгодоприобретателей (при наличии), бенефициарных владельцев клиента-организации в перечне. При нахождении вышеуказанных лиц в перечне, криптобанк отказывает клиенту в установлении договорных отношений с ним.

При идентификации клиента, осуществляющего разовую операцию, криптобанк осуществляет проверку нахождения такого клиента, включая бенефициарных владельцев клиента, в перечне. При нахождении клиента, осуществляющего разовую операцию, бенефициарного владельца клиента в перечне криптобанк блокирует финансовую операцию.

При поступлении денежных средств, цифровых знаков (токенов) клиенту от организации, индивидуального предпринимателя, физического лица, включенных в перечень, криптобанк замораживает поступившие средства и блокирует расходные операции в сумме замороженных средств с даты зачисления этих средств на счет клиента.

При отправлении денежных средств, цифровых знаков (токенов) клиентом, средства которого заморожены, или при отправлении денежных средств и цифровых знаков (токенов) организации, индивидуальному

предпринимателю, физическому лицу, включенным в перечень, криптобанк блокирует финансовую операцию с даты получения криптобанком платежной инструкции клиента на перечисление денежных средств или цифровых знаков (токенов), за исключением финансовых операций, необходимых для обеспечения жизнедеятельности физического лица, индивидуального предпринимателя, на основании решения органа финансового мониторинга при отсутствии наложения ареста на средства клиента в соответствии с частью 3 статьи 132 Уголовно-процессуального кодекса Республики Беларусь.

Уплата вознаграждения по договору займа цифровых знаков (токенов) физического лица, включенного в перечень, и его обязательств по иным гражданско-правовым договорам (оплата жилищно-коммунальных услуг, связи, страхования и др.), налоговым обязательствам, другим обязательным платежам в бюджет осуществляется в безналичной форме поручителями и иными лицами. Осуществление указанных финансовых операций в наличной форме подлежит блокированию. При неисполнении физическим лицом, включенным в перечень, обязательств в рамках займа цифровых знаков (токенов), образовавшаяся просроченная задолженность учитывается на соответствующих счетах с созданием специального резерва на покрытие возможных убытков в соответствии с банковским законодательством.

Криптобанк при верификации сведений о клиентах, их представителях, выгодоприобретателях (при наличии), бенефициарных владельцах клиента-организации и обновлении (актуализации) данных о них в соответствии со статьей 8 Закона № 165-З проводят проверку наличия среди вышеуказанных лиц организаций, физических лиц, в том числе индивидуальных предпринимателей, включенных в перечень. При нахождении клиента, его представителя, выгодоприобретателя (при наличии), бенефициарного владельца клиента-организации в перечне, криптобанк блокирует финансовую операцию, в том числе путем отказа от исполнения договора на осуществление финансовых операций в одностороннем порядке.

Порядок блокирования финансовых операций криптобанк определяет в правилах внутреннего контроля самостоятельно с учетом особенностей осуществляемых финансовых операций в соответствии со статьей 9^1 Закона № 165-З.

Уведомление клиента о запрете на распоряжение, пользование средствами осуществляется путем направления криптобанком письма клиенту без указания причины замораживания этих средств. В случае, предусмотренном в части пятой настоящего пункта, данное письмо направляется также заказчику услуг по размещению цифровых знаков (токенов).

76. Криптобанк информирует собственника или владельца средств, клиента о запрете на осуществление финансовой операции в связи с включением соответствующего лица в перечень при блокировании финансовой операции или после получения письменного обращения от собственника или владельца средств, клиента в срок не позднее 5 рабочих дней с даты получения такого обращения.

77. Криптобанки самостоятельно определяют в своих локальных правовых актах порядок информирования клиента о размораживании средств и (или) разблокировании финансовой операции.

78. Средства, в отношении которых криптобанком применены меры по замораживанию, учитываются криптобанком на счетах и криптоаккаунтах клиентов либо на счетах и криптоаккаунтах, предназначенных для учета средств на временной основе.

ГЛАВА 6
ВЫЯВЛЕНИЕ ФИНАНСОВЫХ ОПЕРАЦИЙ, ПОДЛЕЖАЩИХ ОСОБОМУ КОНТРОЛЮ

79. Выявление в деятельности клиентов финансовых операций, подлежащих особому контролю, осуществляется криптобанком на стадии текущего и последующего контроля в зависимости от итоговой степени риска работы с клиентом:

по клиентам, работе с которыми присвоена низкая или средняя итоговая степень риска, – на стадии последующего контроля;

по клиентам, работе с которыми присвоена высокая итоговая степень риска, – на стадиях текущего и последующего контроля.

Выявление в деятельности клиентов финансовых операций, определенных в абзаце четвертом части первой статьи 7 Закона № 165-З, осуществляется на стадии текущего контроля независимо от присвоенной степени риска работы с клиентом.

При наличии на стадии осуществления финансовой операции подозрений, что она осуществляется в целях получения и (или) легализации доходов, полученных преступным путем, финансирования террористической деятельности, распространения или финансирования распространения оружия массового поражения, криптобанк независимо от присвоенной работе с клиентом итоговой степени риска осуществляет свои действия в порядке, предусмотренном пунктом 87 настоящего Положения.

Криптобанк предусматривает в правилах внутреннего контроля случаи и порядок использования программного обеспечения и (или) иных технологических средств для процессов мониторинга и выявления финансовых операций, подлежащих особому контролю.

80. Криптобанк включает в правила внутреннего контроля критерии выявления и признаки подозрительных финансовых операций:

при осуществлении банковских операций – с учетом перечня осуществляемых банковских операций и Рекомендаций № 113;

по операциям с цифровыми знаками (токенами) – установленные приложением 5 к Положению о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий.

С учетом масштабов деятельности, состава и объема осуществляемых банковских операций и операций с цифровыми знаками (токенами) криптобанк выбирает относящиеся к его деятельности критерии выявления и признаки подозрительных финансовых операций.

Критерии выявления и признаки подозрительных финансовых операций не применяются в отношении финансовых операций клиентов криптобанка, связанных с обеспечением расчетов по внешнеторговым договорам в период действия мер ограничительного характера (международных санкций).

81. Криптобанк в правилах внутреннего контроля вправе конкретизировать и дополнять критерии выявления и признаки подозрительных финансовых операций. При этом, если в признаке подозрительных финансовых операций установлена пороговая сумма, криптобанк вправе ее корректировать в сторону уменьшения.

При конкретизации и дополнении критериев выявления и признаков подозрительных финансовых операций в целях ПОД/ФТ криптобанк использует типологии выявления подозрительных финансовых операций, доводимые Секретариатом Наблюдательного совета ПВТ, Национальным банком, Департаментом финансового мониторинга Комитета государственного контроля, а также собственные разработки.

Криптобанк уведомляет Секретариат Наблюдательного совета ПВТ и Национальный банк об установлении в правилах внутреннего контроля конкретизированных и дополнительных критериев выявления и признаков подозрительных финансовых операций, не предусмотренных в Рекомендациях № 113 и в приложении 5 к Положению о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий, которые в том числе могут являться основанием для отказа клиенту в осуществлении финансовой операции, обосновании внесенных изменений в течение пяти рабочих дней со дня утверждения правил внутреннего контроля (внесения изменений в них) по форме согласно приложению 5.

82. Для отнесения финансовой операции, вызывающей подозрения, к финансовой операции, подлежащей особому контролю, криптобанк руководствуется:

критериями выявления и признаками подозрительных финансовых операций, определенными правилами внутреннего контроля;

анализируемым периодом, установленным в правилах внутреннего контроля для соответствующего критерия выявления и признака подозрительных финансовых операций;

данными о количестве однотипных операций, осуществленных за анализируемый период;

сведениями, полученными из открытых источников информации, характеризующими статус и деятельность клиента, осуществляющего операцию, а также его контрагента;

данными, полученными в ходе идентификации и верификации в отношении клиента;

сведениями о проводимой финансовой операции, необходимыми для понимания сути и деталей осуществления финансовой операции;

сведениями об осуществленных за предыдущий период финансовых операциях с целью подтверждения оснований отнесения либо неотнесения проводимой финансовой операции к подлежащей особому контролю;

информацией, полученной от банка-корреспондента, криптобанка-корреспондента в отношении деловой репутации контрагента клиента и сути проводимых финансовых операций.

83. Криптобанк вправе принять решение о приостановлении и (или) отказе клиенту в осуществлении финансовой операции (за исключением зачисления на счет получателя поступивших денежных средств), об отказе в подключении к системе дистанционного обслуживания, о прекращении или приостановлении оказания услуг посредством этой системы, если финансовая операция отвечает критериям выявления и признакам подозрительных финансовых операций, определенным пунктом 6 Рекомендаций №113, а также критериям, указанным в пунктах 2 – 5, 7, 10 – 12, 14, 17 и 20 приложения 5 к Положению о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий.

При выявлении финансовой операции, отвечающей критериям выявления и признакам подозрительных финансовых операций, указанным в пунктах 18, 21 и 22 приложения 5 к Положению о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий, криптобанк обязан принять решение о приостановлении и (или) отказе в осуществлении такой финансовой операции.

84. Для выявления финансовой операции, отвечающей критериям выявления и признакам подозрительных финансовых операций, предусмотренным пунктом 18 приложения 5 к Положению о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий, криптобанк обязан использовать программные средства[1], обеспечивающие

[1] К программным средствам, указанным в части первой пункта 84 настоящего Положения, относятся программные средства, право на использование которых получено криптобанком от резидентов ПВТ, осуществляющих деятельность KYT-провайдера, или от компаний Chainalysis, Inc. (США), Elliptic Enterprises Limited (Великобритания), Lukka, Inc. (США) либо от иных юридических лиц, правомерно распространяющих

определение характеристик адресов (идентификаторов) виртуальных кошельков (сущностей), отражающих характер их использования и (или) предполагаемых их владельцев, мониторинг и анализ использования адресов (идентификаторов) виртуальных кошельков и определение (визуализацию) их связей с иными адресами (идентификаторами) виртуальных кошельков (граф транзакций), а также осуществляющие оценку риска использования адресов (идентификаторов) виртуальных кошельков, в том числе риска их использования в противоправной деятельности. При использовании названных программных средств криптобанк обязан применять в том числе программные инструменты для определения (визуализации) связей адресов (идентификаторов) виртуальных кошельков с иными адресами (идентификаторами) виртуальных кошельков (граф транзакций), а также предусмотреть в правилах внутреннего контроля случаи, при которых применение таких программных инструментов является обязательным.

Обязанность, предусмотренная частью первой настоящего пункта, не распространяется на сделки (операции) с цифровыми знаками (токенами) в отношении которых компании, поименованные в части первой настоящего пункта, не предоставляют (не поддерживают) возможность обобщения и анализа транзакций в соответствующих реестрах блоков транзакций (блокчейнах), а равно использования адресов (идентификаторов) виртуальных кошельков, на которых находятся такие цифровые знаки (токены).

При этом к числу данных цифровых знаков (токенов) не относятся цифровые знаки (токены), в основе которых лежит принцип полной анонимизации совершаемых с ними сделок (операций).

85. Криптобанки вправе отказаться в одностороннем порядке от исполнения договора на осуществление финансовых операций в письменной форме при наступлении обстоятельств, определенных в абзаце четвертом части шестой подпункта 4.1 пункта 4 Декрета № 8.

86. Документальное фиксирование финансовых операций, подлежащих особому контролю, осуществляется в соответствии с пунктом 8 приложения к постановлению № 1249.

87. При выявлении финансовой операции, вызывающей подозрения, работником криптобанка составляется сообщение в электронном виде, содержащее сведения об осуществляемой финансовой операции по форме, утвержденной криптобанком.

Сообщение включает следующие сведения о финансовой операции:

наименование (фамилия, инициалы) клиента;

программные средства, разработчиками (правообладателями) которых являются вышепоименованные компании, или от иных юридических лиц при условии, что предоставляемые такими лицами программные средства имеют тот же или более высокий уровень эффективности, что и программные средства, разработчиками (правообладателями) которых являются вышепоименованные компании.

вид финансовой операции;

наименование (фамилия, инициалы) контрагента;

сумма финансовой операции;

основание отнесения финансовой операции к вызывающей подозрения;

подпись, фамилия, инициалы и должность сотрудника, составившего сообщение;

дата составления сообщения;

резолюция ответственного должностного лица криптобанка о признании (непризнании) финансовой операции подозрительной и обоснование принятого решения.

Данное сообщение, а также необходимые документы по финансовой операции передаются ответственному должностному лицу криптобанка.

При необходимости работник или ответственное должностное лицо криптобанка обращаются к клиенту с просьбой о представлении разъяснений об экономическом смысле финансовой операции.

88. При наличии (отсутствии) обоснованных подозрений для отнесения финансовой операции клиента к подлежащей особому контролю ответственное должностное лицо криптобанка принимает мотивированное решение о признании финансовой операции клиента подозрительной (неподозрительной) и представлении (непредставлении) сведений о ней в орган финансового мониторинга.

При принятии такого решения в отношении осуществляемой клиентом финансовой операции, являющейся одной из однотипных финансовых операций, криптобанк:

в случае ее признания подозрительной в целях дальнейшего представления специальных формуляров по таким операциям руководствуется анализируемым периодом, установленным в правилах внутреннего контроля для соответствующего признака подозрительности. При необходимости ответственное должностное лицо вправе принять решение об иной периодичности проведения анализа однотипных финансовых операций клиента в зависимости от их суммы, вида, характера и частоты осуществления;

в случае ее признания неподозрительной ответственное должностное лицо вправе принять решение о дальнейшем не составлении сообщений по таким операциям при незначительных изменениях в сумме, виде, характере и частоте их осуществления в дальнейшем (при отсутствии соответствия другим критериям выявления и признакам подозрительных финансовых операций).

По однотипным финансовым операциям решение о признании их подозрительными (неподозрительными) принимается не позднее девяти рабочих дней, следующих за последним днем анализируемого периода.

89. В случае признания ответственным должностным лицом криптобанка финансовой операции неподозрительной им принимается и фиксируется в сообщении обоснование решения о признании финансовой операции неподозрительной.

Сообщения, по которым принято решение о ненаправлении специального формуляра, регистрируются в журнале учета сообщений, форма которого определяется криптобанком самостоятельно. Ведение журнала учета сообщений осуществляется в электронном виде.

Если ответственное должностное лицо криптобанка принимает решение о признании финансовой операции подозрительной, соответствующая запись о принятом решении в сообщении не оформляется. Обоснованием принятого решения о признании операции подозрительной является подписание ответственным должностным лицом специального формуляра регистрации финансовых операций, подлежащих особому контролю.

90. Финансовые операции, подлежащие особому контролю, регистрируются в специальном формуляре регистрации финансовых операций, подлежащих особому контролю, в порядке, установленном Инструкцией о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю, утвержденной постановлением Совета Министров Республики Беларусь от 16 марта 2006 г. №367.

91. При выявлении подозрительной финансовой операции ответственное должностное лицо криптобанка при необходимости принимает следующие решения:

о запросе дополнительных документов (сведений), их анализе, в том числе путем сопоставления содержащейся в них информации с информацией, имеющейся в распоряжении криптобанка;

о пересмотре степени риска работы с клиентом;

об отказе в одностороннем порядке от исполнения договора на осуществление финансовых операций в письменной форме в соответствии с законодательством;

другие решения, принимаемые в отношении участника финансовой операции, перечень которых при необходимости определяется криптобанком в соответствии с настоящим Положением в правилах внутреннего контроля.

92. Криптобанк информирует клиента о приостановлении им финансовой операции, об отказе в ее осуществлении, отказе в подключении клиента к системе дистанционного обслуживания, о прекращении или приостановлении оказания услуг посредством такой системы, об отказе в одностороннем порядке от исполнения договора на осуществление финансовых операций в письменной форме в порядке,

установленном правилами внутреннего контроля, в соответствии с частью пятой статьи 6 Закона № 165-З.

93. Исполнение решений органа финансового мониторинга о приостановлении и возобновлении финансовых операций осуществляется в порядке, предусмотренном постановлением Совета Министров Республики Беларусь от 23 ноября 2016 г. № 954 ”Об утверждении Положения о порядке приостановления и возобновления финансовых операций органом финансового мониторинга, взаимодействия органа финансового мониторинга с лицами, осуществляющими финансовые операции“.

94. Криптобанк обеспечивает путем определения в организационно-распорядительных или локальных правовых актах, должностных лиц, ответственных за:

надлежащее хранение анкет клиентов, электронных копий специальных формуляров и копий, изображений иных документов, связанных с осуществлением финансовых операций, подлежащих особому контролю, в течение срока, установленного настоящим Положением и законодательством;

соблюдение установленного законодательством порядка обращения с информацией о финансовых операциях и идентификационными данными участников финансовой операции.

ГЛАВА 7
ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ, ДЕЛОВОЙ РЕПУТАЦИИ И ПОДГОТОВКЕ РАБОТНИКОВ КРИПТОБАНКА

95. Работникам подразделения комплаенс-контроля необходимо наличие высшего образования и опыта работы в подразделении банка, входящем в организационную структуру системы внутреннего контроля банка, криптобанка, оператора криптоплатформы, оператора обмена криптовалют, оператора зарубежной торговой площадки, не менее шести месяцев, а при отсутствии высшего образования – наличие опыта работы в сфере ПОД/ФТ не менее одного года или опыта работы в подразделении банка, входящем в организационную структуру системы внутреннего контроля банка, криптобанка, не менее одного года.

96. Руководитель подразделения комплаенс-контроля, лицо, его замещающее, должны соответствовать квалификационным требованиям и требованиям к деловой репутации, определенным соответственно частью пятой пункта 22 и пунктом 23 Инструкции о порядке проведения Национальным банком оценки соответствия квалификационным требованиям и требованиям к деловой репутации, об аттестации и специальной аттестации, утвержденной постановлением Правления Национального банка Республики Беларусь от 19 декабря 2012 г. № 669.

Ответственные должностные лица должны отвечать квалификационным требованиям, предусмотренным в абзаце четвертом пункта 6 Положения о требованиях, которым должны соответствовать заявители, планирующие осуществлять деятельность криптобанка, и требованиях к их бизнес-проектам, утвержденного решением Наблюдательного совета Парка высоких технологий (протокол от 29 июня 2026 г. № 3).

97. Работники криптобанков в случаях, предусмотренных настоящим Положением, должны проходить инструктаж по вопросам ПОД/ФТ.

Порядок проведения инструктажа по вопросам ПОД/ФТ определяется криптобанком с учетом требований настоящего Положения и должен включать, в числе прочего, порядок проверки знаний соответствующих работников криптобанка в сфере ПОД/ФТ.

98. Инструктаж может быть вводным (первичным), плановым (обучение) и внеплановым (целевым).

99. Вводный (первичный) инструктаж и ознакомление с нормативными правовыми актами Республики Беларусь, локальными правовыми актами криптобанка, нормативными правовыми актами Национального банка, актами Наблюдательного совета ПВТ по вопросам ПОД/ФТ проводится с лицами, назначаемыми на должности ответственного должностного лица, руководителя и работника подразделения комплаенс-контроля по вопросам ПОД/ФТ, лицами, принимаемыми на работу в подразделения, участвующие в осуществлении финансовых операций, в течение 10 рабочих дней с даты назначения (приема).

100. Плановый инструктаж (обучение) ответственных должностных лиц, руководителя и работников подразделения комплаенс-контроля по вопросам ПОД/ФТ, работников криптобанка, участвующих в осуществлении финансовых операций, проводится не реже одного раза в год.

При проведении планового инструктажа (обучения), предусмотренного в части первой настоящего пункта, могут использоваться обучающие курсы, в том числе дистанционные.

101. Внеплановый (целевой) инструктаж по вопросам ПОД/ФТ проводится в следующих случаях:

при изменении законодательства в сфере ПОД/ФТ, получении информационных документов по вопросам ПОД/ФТ из государственных органов, Секретариата Наблюдательного совета ПВТ;

при изменении правил внутреннего контроля (при необходимости и в части соответствующих изменений);

при выявлении в ходе проверок по вопросам ПОД/ФТ нарушений либо недостатков в работе криптобанка;

при возложении на работника криптобанка функций, предусмотренных пунктом 10 настоящего Положения, либо функций, связанных с осуществлением финансовых операций;

при выходе ответственного должностного лица, руководителя и работников подразделения комплаенс-контроля по вопросам ПОД/ФТ, работников криптобанка, участвующих в осуществлении финансовых операций, из длительного отпуска либо в случае их явки на работу по окончании длительного периода временной нетрудоспособности, если криптобанк придет к выводу, что имеющихся у них знаний в сфере ПОД/ФТ недостаточно для дальнейшего выполнения ими своих трудовых обязанностей;

в иных случаях, определяемых криптобанком, в том числе в случае, предусмотренном в пункте 102 настоящего Положения.

102. Ответственное должностное лицо организует проверку знаний по вопросам ПОД/ФТ у работников криптобанка, участвующих в осуществлении финансовых операций, не реже одного раза в год. В случае неудовлетворительного результата в отношении релевантного работника может быть проведен внеплановый (целевой) инструктаж по вопросам ПОД/ФТ и (или) приняты иные меры, определяемые криптобанком в соответствии с законодательством.

103. Факты проведения инструктажа и проверки знаний фиксируются в специальном журнале, форму и содержание которого криптобанк устанавливает самостоятельно, и подтверждаются подписью работника, в отношении которого проведен инструктаж или проведена проверка знаний. Указанный журнал может заполняться в электронном виде, и в этом случае подпись названного работника не требуется.

104. Проверка знаний ответственного должностного лица, руководителя и работников подразделения комплаенс-контроля по вопросам ПОД/ФТ, работников криптобанка, участвующих в осуществлении финансовых операций, по вопросам ПОД/ФТ должна проводиться не реже одного раза в год, а первичная проверка знаний – в течение одного месяца со дня проведения вводного (первичного) инструктажа.

Приложение 1
к Положению о требованиях к правилам внутреннего контроля криптобанков

АНКЕТА ОТВЕТСТВЕННОГО ДОЛЖНОСТНОГО ЛИЦА В ЧАСТИ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПО ПРЕДОТВРАЩЕНИЮ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, ФИНАНСИРОВАНИЯ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ И ФИНАНСИРОВАНИЯ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ

I. Общие сведения об ответственном должностном лице в части выполнения требований по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения (далее – легализация)

_____

фамилия, собственное имя, отчество (если таковое имеется) ответственного должностного лица в части выполнения требований по предотвращению легализации

_____

указать предыдущие фамилии (в случае изменения фамилии)

_____

дата рождения ответственного должностного лица в части выполнения требований по предотвращению легализации

_____

гражданство ответственного должностного лица в части выполнения требований по предотвращению легализации

_____

место жительства должностного лица в части выполнения требований по предотвращению легализации

_____

контактный телефон и адрес электронной почты должностного лица в части выполнения требований по предотвращению легализации

II. Сведения о соответствии (несоответствии) ответственного должностного лица в части выполнения требований по предотвращению легализации требованиям к деловой репутации и иные сведения о нем

№	Вопрос	Ответ
1.	Имеется ли у ответственного должностного лица в части выполнения требований по предотвращению легализации высшее образование (если имеется, то указать учреждение высшего образования, год его окончания, факультет и специальность по диплому)?	
2.	Имеется ли у ответственного должностного лица в части выполнения требований по предотвращению легализации опыт работы по экономической или юридической специальности не менее трех лет или стаж работы не менее двух лет в качестве лица, в обязанности которого входит реализация мер по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения (если имеется, то указать какой и где именно он имел место)?	
3.	Имеется ли у ответственного должностного лица в части выполнения требований по предотвращению легализации непогашенная или неснятая судимость в Республике Беларусь и государстве (государствах), гражданином (подданным) которого (которых) он является?	
4.	Имеются ли у ответственного должностного лица в части выполнения требований по предотвращению легализации в течение последних двух лет факты расторжения трудового договора (контракта) по инициативе нанимателя по причине совершения данным должностным лицом виновных действий, являющихся основаниями для утраты доверия к работнику со стороны нанимателя, в Республике Беларусь?	
5.	Имеются ли у ответственного должностного лица в части выполнения требований по предотвращению легализации в течение последних двух лет факты расторжения трудового договора (контракта) по основаниям, признаваемым дискредитирующими обстоятельствами увольнения в соответствии с пунктом 6 Декрета Президента Республики Беларусь от 15 декабря 2014 г. № 5 ”Об усилении требований к руководящим кадрам и работникам организаций“, в Республике Беларусь?	
6.	Имеется ли в течение последних трех лет вступившее в законную силу решение суда, которым установлены факты осуществления ответственным должностным лицом в части выполнения требований по предотвращению легализации виновных действий, повлекших банкротство юридического лица, в Республике Беларусь и государстве (государствах), гражданином (подданным) которого (которых) он является?	
7.	Имеется ли постановление органа уголовного преследования Республики Беларусь или государства, гражданином (подданным) которого является ответственное должностное лицо в части выполнения требований по предотвращению легализации, о возбуждении в отношении него уголовного дела, либо о признании его подозреваемым, либо о привлечении его в качестве обвиняемого по уголовному делу?	

_____
дата подписания анкеты

_____подпись, фамилия,
инициалы, должность лица, подписавшего анкету от имени заявителя

_____
подпись, фамилия, инициалы ответственного должностного лица в части выполнения требований по предотвращению легализации

Приложение 2

к Положению о требованиях к правилам внутреннего контроля криптобанков

ПЕРЕЧЕНЬ СВЕДЕНИЙ ДЛЯ ВКЛЮЧЕНИЯ В ОТЧЕТ О ВНУТРЕННЕЙ ОЦЕНКЕ РИСКОВ, СВЯЗАННЫХ С ЛЕГАЛИЗАЦИЕЙ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, ФИНАНСИРОВАНИЕМ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ И ФИНАНСИРОВАНИЕМ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ

1. Методология проведения оценки рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения.

2. Перечень локальных правовых актов, регламентирующих деятельность резидента ПВТ в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения.

3. Сведения об оценке рисков резидента ПВТ в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения:

динамика количества клиентов;

динамика количества клиентов, отнесенных к высокой группе риска;

динамика количества клиентов – публичных должностных лиц;

динамика количества клиентов – организаций, бенефициарными владельцами которых являются лица, отнесенные к публичным должностным лицам.

динамика количества отказов клиентам в осуществлении финансовых операций;

динамика количества специальных формуляров, направленных в орган финансового мониторинга;

перечень услуг, предоставляемых резидентом ПВТ, с высоким уровнем рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения;

количество клиентов в разрезе топ-5 юрисдикций;

общая сумма финансовых операций клиентов в разрезе топ-5 юрисдикций с наибольшей суммой сделок;

4. Меры, принятые органами, ведущими уголовный процесс, по наложению ограничений на средства клиентов.

5. Анализ проверок деятельности в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, проведенных уполномоченными органами, внешним аудитом, иными подразделениями резидента ПВТ (служба внутреннего аудита, служба внутреннего контроля), ответственным должностным лицом за период деятельности резидента ПВТ:

количество проверок;

выявленные нарушения и недостатки;

рекомендации по результатам проверок;

меры воздействия, принятые к лицам, допустившим нарушения;

принятые меры по устранению нарушений и созданию условий для их недопущения в будущем, реализации рекомендаций по результатам проверок.

6. Оценка рисков, связанных с финансированием террористической деятельности.

Количество случаев и суммы замораживания средств и (или) блокирования финансовых операций.

7. Уязвимости и выявленные риски, связанные с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения в деятельности резидента ПВТ.

8. Основные итоги региональной, национальной, секторальной в соответствующей области деятельности оценок рисков, в том числе имеющиеся данные о преступлениях, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения.

Влияние итогов оценок на риски, выявленные резидентом ПВТ.

9. Предложения об ограничении (снижении) рисков, связанных с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения, в деятельности резидента ПВТ и меры по повышению эффективности работы в указанной сфере.

10. Иные сведения.

Приложение 3
к Положению о требованиях к
правилам внутреннего контроля
криптобанков

МАТРИЦА ПРИСВОЕНИЯ РАБОТЕ С КЛИЕНТОМ ИТОГОВОЙ СТЕПЕНИ РИСКА НА ОСНОВЕ ТРЕХВЕКТОРНОЙ МОДЕЛИ РАСПРЕДЕЛЕНИЯ РИСКОВ

Значение векторов			Итоговая степень риска работы с клиентом
Риск по профилю клиента	Риск по географическому региону	Риск по видам операций	
низкий	низкий	низкий	низкий
низкий	низкий	средний	низкий
низкий	низкий	высокий	низкий
низкий	средний	низкий	низкий
низкий	средний	средний	низкий
низкий	средний	высокий	средний
низкий	высокий	низкий	низкий
низкий	высокий	средний	средний
низкий	высокий	высокий	средний
средний	низкий	низкий	низкий
средний	низкий	средний	средний
средний	низкий	высокий	средний
средний	средний	низкий	средний
средний	средний	средний	средний
средний	средний	высокий	средний
средний	высокий	низкий	средний
средний	высокий	средний	средний
средний	высокий	высокий	высокий
высокий	низкий	низкий	средний
высокий	низкий	средний	средний
высокий	низкий	высокий	высокий
высокий	средний	низкий	средний
высокий	средний	средний	высокий
высокий	средний	высокий	высокий
высокий	высокий	низкий	высокий
высокий	высокий	средний	высокий
высокий	высокий	высокий	высокий

Приложение 4

к Положению о требованиях к правилам внутреннего контроля криптобанков

ПЕРЕЧЕНЬ ДОПОЛНИТЕЛЬНЫХ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ

1. Для физического лица:

учетный номер плательщика (на основании документа, подтверждающего постановку на учет в налоговом органе) (при наличии);

место работы, должность, номер рабочего телефона (при наличии);

номер контактного (домашнего/мобильного) телефона;

предыдущие фамилии (при регистрации рождения, заключения брака(ов) и др.) (при наличии);

адрес сайта в глобальной компьютерной сети Интернет (при наличии);

сведения о представителях, лицах, способных прямо и (или) косвенно (через иных лиц) определять (оказывать влияние на принятие) решения физического лица, о лицах, на принятие решений, которыми физическое лицо оказывает такое влияние (при наличии);

иные сведения, определенные в правилах внутреннего контроля.

2. Для индивидуального предпринимателя:

номер контактного (домашнего/мобильного) телефона;

адрес сайта глобальной компьютерной в сети Интернет (при наличии);

предыдущие фамилии (при регистрации рождения, заключении брака(ов) и др.) (при наличии);

предполагаемые среднемесячные обороты по счету (общие и обороты наличных денежных средств);

сведения о представителях, лицах, способных прямо и (или) косвенно (через иных лиц) определять (оказывать влияние на принятие) решения индивидуального предпринимателя, о лицах, на принятие решений, которыми индивидуальный предприниматель оказывает такое влияние;

иные сведения, определенные в правилах внутреннего контроля.

3. Для организаций:

номера контактных телефонов;

адрес сайта в глобальной компьютерной сети Интернет (при наличии);

размер зарегистрированного уставного фонда;

количество работников, трудоустроенных у соответствующего нанимателя на дату получения данных об их количестве;

сведения о постоянных контрагентах (при наличии);

сведения о представителях;

история организации, положение на рынке (сведения о реорганизациях, изменениях в характере деятельности);

информация о том, являются ли руководители, главный бухгалтер организации и (или) иные уполномоченные должностные лица, которым в установленном порядке предоставлено право действовать от имени организации, учредителями (участниками) других организаций с долей в уставном фонде более 25 процентов или собственниками других организаций (сведения об этих организациях);

информация о том, являются ли учредители (участники) организации, имеющие долю в уставном фонде более 25 процентов, собственники или бенефициарные владельцы учредителями (участниками) других организаций с долей в уставном фонде более 25 процентов, собственниками или руководителями других организаций (сведения об этих организациях);

сведения о филиалах, представительствах, дочерних организациях (в том числе за границей) (при наличии);

сведения об организациях, способных прямо и (или) косвенно (через иные организации) определять решения данной организации или оказывать влияние на их принятие данной организацией, а также об организациях, на принятие решений, которыми данная организация оказывает такое влияние;

иные сведения, определенные в правилах внутреннего контроля.

Приложение 5
к Положению о требованиях к
правилам внутреннего
контроля криптобанков

Форма

ИНФОРМАЦИЯ
об установлении в правилах внутреннего контроля криптобанка конкретизированных и дополнительных критериев выявления и признаков подозрительных финансовых операций

N п/п	Код <*>	Описание критерия выявления и признака подозрительных финансовых операций	Описание конкретизированного и дополнительного критериев выявления и признака подозрительных финансовых операций	Обоснование корректировки критерия выявления и признака подозрительных финансовых операций, введения дополнительного критерия

<*> В соответствии с приложением 4 к Инструкции о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю, утвержденной постановлением Совета Министров Республики Беларусь от 16 марта 2006 г. N 367.