Правила внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в АКБ «ASIA ALLIANCE BANK»

Ташкент-2023

СОДЕРЖАНИЕ

I	**ОБЩИЕ ПОЛОЖЕНИЯ**	**2-5**
II	**НАДЛЕЖАЩАЯ ПРОВЕРКА КЛИЕНТОВ**	**5-17**
III	**ПРАВИЛА ОСУЩЕСТВЛЕНИЯ МОНИТОРИНГА ЗА ОПЕРАЦИЯМИ**	**17-26**
IV	**ПОРЯДОК ВЫЯВЛЕНИЯ, ОЦЕНКИ, УПРАВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ УРОВНЯ РИСКА**	**26-30**
V	**ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ КЛИЕНТОВ**	**30-33**
VI	**ПОРЯДОК КОНТРОЛЯ НАД ОПЕРАЦИЯМИ ЛИЦ, ВКЛЮЧЕННЫХ В ПЕРЕЧЕНЬ**	**33-36**
VII	**ОФОРМЛЕНИЕ, ХРАНЕНИЕ, ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ И ДОКУМЕНТОВ, ПОЛУЧЕННЫХ В РЕЗУЛЬТАТЕ ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ**	**36-39**
VIII	**КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ К ПОДГОТОВКЕ И ОБУЧЕНИЮ КАДРОВ ВНУТРЕННЕГО КОНТРОЛЯ**	**39-41**
IX	**ВЗАИМООТНОШЕНИЕ СЛУЖБЫ ВНУТРЕННЕГО КОНТРОЛЯ С ДРУГИМИ ПОДРАЗДЕЛЕНИЯМИ БАНКА**	**41-43**
X	**ОСУЩЕСТВЛЕНИЕ КОНТРОЛЯ НАД ИСПОЛНЕНИЕМ ПРАВИЛ ВНУТРЕННЕГО КОНТРОЛЯ**	**43-45**

I.ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила разработаны в соответствии с законами Республики Узбекистан «О банках и банковской деятельности», от 30 августа 2003 года «О банковской тайне», «О противодействии легализации доходов, полученных от преступной деятельности, и финансированию терроризма»; «Положением о порядке представления сведений связанных с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма» (приложение № 1 к Постановлению Кабинета Министров Республики Узбекистан от 29 июня 2021 года № 402), «Правилами внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в коммерческих банках» (далее – Правила внутреннего контроля), зарегистрированными 23 мая 2017 года в Министерстве юстиции за № 2886, «Положение о цифровой идентификации клиентов», зарегистрированными 30 сентября 2021 года в Министерстве юстиции за № 3322, «Положением о порядке приостановления операций, замораживания денежных средств или иного имущества, предоставления доступа к замороженному имуществу и возобновления операций лиц, включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения», зарегистрированным 19 октября 2021 года в Министерстве юстиции за № 3327.

Настоящие правила определяют порядок организации и осуществления внутреннего контроля с целью противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «ASIA ALLIANCE BANK» (далее – Банк), в также порядок приостановления операций, замораживания денежных средств или иного имущества, предоставления доступа к замороженному имуществу и возобновления операций лиц, включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения.

2. В настоящих Правилах используются следующие основные понятия:

внутренний контроль — деятельность коммерческого банка по надлежащей проверке клиентов, управлению рисками легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения, выявлению сомнительных и подозрительных операций, а также операций, участниками которых являются лица, участвующие или подозреваемые в участии в террористической деятельности или распространении оружия массового уничтожения;

система внутреннего контроля – совокупность действий Службы внутреннего контроля и других подразделений коммерческого банка, направленных на достижение целей и выполнение задач, определенных настоящими Правилами и внутренними документами;

Служба внутреннего контроля — специальное подразделение коммерческого банка, ответственное за осуществление внутреннего контроля;

сотрудники Службы внутреннего контроля – сотрудники Службы внутреннего контроля головного офиса коммерческого банка, ответственный сотрудник или руководитель и сотрудники Службы внутреннего контроля филиала коммерческого банка, ответственные за осуществление внутреннего контроля;

руководитель Службы внутреннего контроля – начальник Управления внутреннего контроля непосредственно контролирующий осуществление деятельности системы внутреннего контроля в банке на основании правил внутреннего контроля, являющийся руководителем сотрудников Службы внутреннего контроля;

специально уполномоченный государственный орган – Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан (далее – Департамент);

клиент — физическое или юридическое лицо, обратившееся в коммерческий банк с поручением (заявлением, ходатайством) об осуществлении операции с денежными средствами или иным имуществом (далее — операции);

бенефициарный собственник – лицо, которое в конечном итоге владеет правами собственности или реально контролирует клиента, и в интересах которого совершается операция с денежными средствами или иным имуществом;

сомнительная операция – операция, в отношении которой у коммерческого банка в процессе осуществления внутреннего контроля возникло сомнение об ее осуществлении с целью легализации доходов, полученных от преступной деятельности, финансирования терроризма и (или) финансирования распространения оружия массового уничтожения, до принятия решения о включении (невключении) ее в категорию подозрительных операций;

подозрительная операция – операция, находящаяся в процессе подготовки, совершения или уже совершенная, в отношении которой у коммерческого банка в процессе осуществления внутреннего контроля возникло подозрение об ее осуществлении с целью легализации доходов, полученных от преступной деятельности, финансирования терроризма и (или) финансирования распространения оружия массового уничтожения;

разовые операции – операции, осуществляемые клиентами в разовом порядке без открытия банковского счета, не повторяющиеся, по меньшей мере, в течение одного месяца;

надлежащая проверка клиента – проверка личности и полномочий клиента и лиц, от имени которых он действует, идентификация бенефициарного собственника клиента, а также проведение на постоянной основе изучения деловых отношений и операций, осуществляемых клиентом, в целях проверки их соответствия сведениям о таком клиенте и его деятельности;

идентификация клиента – определение коммерческим банком данных о клиентах на основе предоставленных ими документов, дополнительно подтвержденных сведений, доступных в открытых источниках и базах данных в целях осуществления надлежащей проверки клиента;

идентификация бенефициарного собственника клиента – определение коммерческим банком юридического лица собственника, в том числе лица контролирующего клиента путем изучения структуры собственности и управления на основании учредительных документов, определенных законодательством (устава и (или) учредительного договора, положения);

государства, не участвующие в международном сотрудничестве в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма – государства и территории, определенные в официальных заявлениях Группы по разработке финансовых мер борьбы с отмыванием денег, которые представляют угрозу международной финансовой системе и у которых система противодействия легализации доходов, полученных от преступной деятельности и финансированию терроризма, имеет стратегические недостатки;

оффшорная зона - государства и территории, предоставляющие льготный налоговый режим и (или) не предусматривающие раскрытие и представление информации при проведении финансовых операций;

риск - риск совершения клиентами операций в целях легализации доходов, полученных от преступной деятельности, финансирования терроризма или финансирования распространения оружия массового уничтожения;

дистанционные услуги - банковские услуги, предоставляемые по проведению операций с использованием программ, дающих возможность осуществления операций без явки клиента в Банк.

публичные должностные лица – лица, назначаемые или избираемые постоянно, временно или по специальному полномочию, выполняющие организационно-распорядительные функции и уполномоченные на совершение юридически значимых действий в законодательном, исполнительном, административном или судебном органе, в

том числе военных структурах иностранного государства либо в международной организации, а также высокопоставленные руководители предприятий иностранных государств, известные политики и известные члены политических партий иностранных государств (включая бывших);

замораживание денежных средств или иного имущества – запрет на перевод, конверсию, распоряжение или перемещение денежных средств или иного имущества;

приостановление операции – приостановление исполнения поручений клиента о переводе, конверсии, передаче во владение и пользование другим лицам денежных средств или иного имущества, а также совершении других юридически значимых действий;

лицо, участвующее или подозреваемое в участии в террористической деятельности – физическое или юридическое лицо, которое участвует или подозревается в участии в террористической деятельности, прямо или косвенно является собственником или контролирует организацию, осуществляющую или подозреваемую в осуществлении террористической деятельности, а также юридическое лицо, которое находится в собственности или под контролем физического лица либо организации, осуществляющих или подозреваемых в осуществлении террористической деятельности;

лицо, участвующее или подозреваемое в участии в распространении оружия массового уничтожения – физическое или юридическое лицо, определенное резолюциями Совета Безопасности ООН и международно-правовыми документами, признанными Республикой Узбекистан, направленными на предотвращение распространения оружия массового уничтожения;

Перечень – перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, формируемый Департаментом на основании сведений, представляемых государственными органами, осуществляющими борьбу с терроризмом, распространением оружия массового уничтожения, и другими компетентными органами Республики Узбекистан, а также сведений, полученных по официальным каналам от компетентных органов иностранных государств и международных организаций.

третья сторона — организации, зарегистрированные в Республике Узбекистан и осуществляющие операции с денежными средствами или иным имуществом, указанные в статье 12 Закона Республики Узбекистан «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения»;

иностранная структура без образования юридического лица — организационная структура, созданная в соответствии с законодательством иностранного государства без образования юридического лица и имеющая право осуществлять деятельность, направленную на извлечение дохода (прибыли) в интересах своих участников (пайщиков, доверителей или иных лиц) либо иных бенефициаров (фонды, партнерства, товарищества, трасты, иные формы осуществления коллективных инвестиций и (или) доверительного управления).

платежный агент — юридическое лицо, не являющееся банком, заключившее с банком или платежной организацией агентский договор на оказание платежных услуг;

платежный субагент — юридическое лицо, не являющееся банком, или индивидуальный предприниматель, заключивший с платежным агентом субагентский договор на оказание платежных услуг;

цифровая идентификация – процесс проверки и проверки личности клиента с использованием информационных систем в соответствии с требованиями, установленными Положением «О цифровой идентификации клиентов»;

цифровая аутентификация - процесс проверки и верификации личности клиента путем автоматизированного (без человеческого фактора) сопоставления фото или видео, снятых в режиме реального времени от ранее идентифицированного клиента, с исходными идентификационными данными;

Контакт-центр (далее Центр) – подразделение Банка или служба, осуществляющая прием-обработку телефонных звонков, SMS и e-mail сообщении, а также сообщения по чатам и социальным сетям или через друге каналы для информирования о продуктах и услугах Банка, и иные функции, определяемые Банком, для обслуживания Клиента;

II.НАДЛЕЖАЩАЯ ПРОВЕРКА КЛИЕНТОВ

2.1. Общие положения по надлежащей проверке клиентов

2.1.1. Надлежащая проверка клиентов является одной из мер направленных на противодействие легализации доходов, полученных от преступной деятельности, и финансированию терроризма. Надлежащая проверка клиентов осуществляется с целью знания на должном уровне, кем и с какой целью осуществляются операции в Банке.

2.1.2. Соответствующие подразделения Банка обязаны самостоятельно принимать меры по надлежащей проверке клиентов в следующих случаях:

а) при установлении хозяйственных и гражданско-правовых отношений, в том числе:

при обращении юридического или физического лица с заявлением на открытие банковского счета (вклада);

при обращении физического лица с заявлением на получение банковской карты;

при обращении юридических и (или) физических лиц с заявлением на приобретение ценных бумаг, эмитированных коммерческим банком;

при владении юридическими и (или) физическими лицами акциями коммерческого банка, на сумму, равную или превышающую один процент его уставного капитала;

при обращении физического лица за получением кредита или услуги по хранению ценностей в банковской депозитной ячейке;

б) при осуществлении разовых операций, в том числе путем совершения одной или нескольких операций, связанных между собой, в случаях:

получения клиентами из банковской кассы наличной иностранной валюты по банковским картам, эмитированным другими банками, на сумму, равную или превышающую 100-кратный размер базовой расчетной величины;

покупки физическими лицами иностранной валюты в размере, превышающем 100 долларов США в эквиваленте;

осуществления операции без открытия или использования банковского счета на сумму, равную или превышающую 500-кратный размер базовой расчетной величины;

при совершении или получении денежных переводов, предусмотренных пунктом 2.6.8 настоящих Правил;

в) при наличии подозрений в легализации доходов, полученных от преступной деятельности, и финансировании терроризма независимо от любых исключений, установленных настоящими Правилами;

г) при наличии сомнений относительно достоверности или достаточности ранее полученных данных о клиенте.

Платежные агенты и платежным субагенты могут проводить проверку личности и идентификацию клиентов в целях применения мер по надлежащей проверки клиента, при соблюдении требований законодательства о противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения, в случаях если это предусмотрено агентским и (или) субагентским договором.

2.1.3. Меры по надлежащей проверке клиента, принимаемые сотрудниками Банка, обязательно включают:

проверку личности и идентификацию клиента;

идентификацию, проверку личности и полномочий лица, действующего от имени клиента, на основании соответствующих документов;

идентификацию бенефициарного собственника клиента;

изучение цели и характера деловых отношений или запланированных операций;

проведение на постоянной основе изучения деловых отношений и операций, осуществляемых клиентом, в целях проверки их соответствия сведениям о таком клиенте и его деятельности, характере риска, в том числе об источнике средств, когда это необходимо.

Банки обязаны использовать системы управления рисками в целях определения того, является ли клиент или бенефициарный собственник публичным должностным лицом и вместе с принятием вышеуказанных мер по надлежащей проверке клиента в отношении публичных должностных лиц, выступающих в качестве клиента или бенефициарного собственника:

применять разумные меры для проверки сведений о статусе публичного должностного лица и определения источника денежных средств или иного имущества по операции;

устанавливать (или продолжать для существующих клиентов) деловые отношения с публичным должностным лицом только с разрешения председателя правления банка или его уполномоченного заместителя;

осуществлять постоянный углубленный мониторинг деловых отношений.

Банк обязаны применять вышеуказанные меры также к членам семей публичных должностных лиц или лицам, близким к публичным должностным лицам.

Банк незамедлительно сообщают Департаменту о связанных с формированием источников денежных средств или иного имущества и запланированных операциях, одновременно имеющих критерии, приведенные в пункте 3.1.2 настоящих Правил, и проводят такие операции в течение не более трех рабочих дней после осуществления полного анализа в целях выявления уровня риска их взаимосвязанности.

2.1.4 В случае обращения юридических лиц и индивидуальных предпринимателей, учредителями которых являются резиденты Республики Узбекистан, с заявлением о дистанционном открытии банковского счета в процессе прохождения их государственной регистрации, меры по надлежащей проверке клиента, предусмотренные в абзаце втором пункта 2.1.3 настоящих Правил, могут быть проведены Центрами государственных услуг (далее — регистрирующий орган) и банк могут доверять результатам проведенных мер. При этом банк должен удостовериться:

в возможности незамедлительного получения необходимую информации по мерам надлежащей проверке клиента через автоматизированную систему государственной регистрации и постановки на учет субъектов предпринимательства;

в соблюдении требований по проведению мер надлежащей проверки клиентов, установленных в актах законодательства, регистрирующим органом.

В случае невыполнения требований, указанных в абзацах втором и третьем настоящего пункта, коммерческие банки самостоятельно проводят меры по надлежащей проверке клиента.

При проведении мер по надлежащей проверке клиентов регистрирующим органом решение о вступлении в деловые отношения с клиентом коммерческий банк принимает самостоятельно, исходя от риска. При этом в оферте договора банковского счета должно быть указано возможность проведения мер по надлежащей проверке клиентов коммерческими банками.

2.1.5 Коммерческие банки могут доверять результатам надлежащей проверки клиента, проведенной третьими сторонами, по мерам надлежащей проверки, указанным в абзацах втором — четвертом пункта 2.1.3 настоящих Правил. В таких случаях конечную ответственность по надлежащей проверке клиента несет коммерческий банк. При этом коммерческие банки должны удостовериться:

в возможности незамедлительного получения (посредством электронных систем) необходимой информации по надлежащей проверке клиентов;

в возможности по запросу незамедлительного получения копий идентификационных данных и других соответствующих документов по надлежащей проверке клиентов;

в том, что третьи стороны руководствуются внутренними правилами по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения.

В случае несоблюдения одного из требований, предусмотренных в абзацах втором — четвертом настоящего пункта, коммерческие банки должны самостоятельно принимать меры по надлежащей проверке клиентов.

Коммерческие банки принимают решение о вступлении в деловые отношения с клиентом самостоятельно, исходя из риска, а также вправе принимать меры по надлежащей проверке.

Коммерческие банки должны оговорить о возможности принятия мер по надлежащей проверке клиентов в договоре и (или) в договоре оферты.

2.1.6 При отнесении клиента или операции, осуществляемой клиентом, к категории высокого уровня риска банка в отношении такого клиента должны применять следующие усиленные меры по надлежащей проверке:

сбор и фиксирование дополнительной подтвержденной информации о клиенте, доступной в открытых источниках и базах данных;

получение от клиента информации об источниках денежных средств или иного имущества по осуществляемым им операциям;

изучение целей запланированных или проведенных данным клиентом операций;

ведение постоянного мониторинга за осуществляемыми операциями данного клиента.

При отсутствии возможности применения усиленных мер по надлежащей проверке клиента, в частности получения от клиента информации об источниках денежных средств или иного имущества по осуществляемым им операциям и (или) изучения целей, запланированных или проведенных данным клиентом операций, банк должен направить сообщение об этом в Департамент и отказаться от вступления в деловые отношения с таким клиентом или от проведения операций такого клиента.

2.1.7 Все документы, позволяющие идентифицировать клиента и других участников операции, обязаны быть в наличии на дату их представления.

2.1.8 При наличии подозрений у сотрудников соответствующих подразделений Банка в достоверности полученных у клиентов информации (документов), необходимо принять меры по проверке (верификации) данной информации (документов). В этих случаях подразделения Банка могут обратиться в соответствующие организации для определения надежности (действительности) информации (документов) о клиентах.

2.1.9 Банк должен применять меры надлежащей проверки в отношении имеющихся клиентов с учетом значимости и рисков, и в соответствующее время проводить надлежащую проверку существующих отношений с учетом того, когда проводились и в целом проводились или не проводились такие проверки, а также достаточности полученных данных.

2.1.10 Повторная идентификация клиента и реального владельца клиента должна быть проведена в случае возникновения сомнений в точности сведений полученных в результате предыдущей идентификации.

2.1.11 При идентификации клиента и бенефициарного собственника клиента банка, в том числе когда он действует через своих платежных агентов и(или) платежных субагентов, обязан сверять полученную информацию с Перечнем, а также со списком государств, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения, формируемыми и предоставляемыми коммерческим банкам Департаментом в установленном законодательством порядке.

В случае выявления в ходе идентификации клиента и бенефициарного собственника клиента лиц, включенных в Перечень, Банк обязан осуществить меры, установленные в

пунктах 6.1.1–6.1.4 настоящих Правил.

2.1.12 Имеющуюся в Банке автоматизированная банковская система (АБС) при внесении идентификационных сведений клиентов в АБС, должна позволить в автоматическом режиме сверить с Перечнем и другими данными в АБС (ООН, Управления по контролю за зарубежными активами Министерства финансов США (OFAC SDN List) и др.), а также определить и сообщить о них. В случае отсутствия возможности для автоматической сверки, сотрудники соответствующего отдела должны сами сверить их с перечнями в электронной таблице.

2.1.13 Банк вправе отказать клиенту в осуществлении операций в следующих случаях:

отсутствия по своему местонахождению (почтовому адресу) органа управления юридического лица или лица, имеющего право действовать от имени юридического лица без доверенности;

предоставления заведомо недостоверных документов или непредставления документов, запрашиваемых в соответствии с законодательством;

в иных случаях, предусмотренных законодательством.

2.1.14 Банку запрещается:

открывать счета (вклады) на анонимных владельцев, то есть без предоставления открывающим счет (вклад) физическим или юридическим лицом документов, необходимых для его идентификации;

открывать счета на явно вымышленные имена, не подтвержденные документально;

открывать счета без личного присутствия лица, открывающего счет, либо его уполномоченного представителя, за исключением случаев, когда банк имеет возможность провести идентификацию клиента на основании ранее представленных документов, действительных и верифицированных на дату идентификации, а также меры по надлежащей проверке клиентов осуществлены регистрирующим органом либо банк на основании биометрических данных, а также коммерческий банк доверяет результатам надлежащей проверки клиентов, проведенной третьей стороной;

устанавливать и продолжать отношения с банками-нерезидентами, не имеющими на территориях государств, в которых они зарегистрированы, физического присутствия и постоянно действующих органов управления;

выпуск ценных бумаг и других финансовых инструментов на предъявителя;

осуществлять услуги по получению и отправке денежных средств в иностранной валюте, в том числе через системы международных денежных переводов, без идентификации клиента;

создавать дочерние банки, филиалы или представительства на территории государств, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

2.1.15 При отсутствии возможности осуществить надлежащую проверку клиента коммерческий банк, в том числе, когда он действует через своих платежных агентов и (или) субагентов, должен сообщить об этом Департаменту и отказаться от вступления в деловые отношения с таким клиентом или проведения операций такого клиента либо прекратить с ним любые деловые отношения.

2.1.16 Начальники соответствующих отделов несут ответственность за обеспечение своевременного и правильного осуществления надлежащей проверки клиентов и заполнения и электронных анкет.

Управляющие филиалов несут ответственность за осуществление контроля по надлежащей проверке клиентов и заполнение их электронных анкет.

2.2. Идентификация физических лиц

2.2.1. Идентификация клиента — физического лица соответствующее подразделениями Банка проводится на основании документа (паспорта или заменяющего

его документа) удостоверяющего личность, или биометрических данных. При этом банк при идентификации клиента — физического лица:

на основании документа (паспорта или заменяющего его документа), удостоверяющего личность должна ознакомиться с оригиналом такого документа;

на основании биометрических данных, должна провести верификацию таких данных с информационной системой Министерства внутренних дел Республики Узбекистан.

Информация, полученная в результате идентификации физического лица - клиента, вносится в электронную анкету в день совершения операции.

2.2.2. Идентификация клиента - физического лица в Банке осуществляется на основе информации, предусмотренной приложениями № 1 к настоящим Правилам, а также документов, являющихся основанием совершения операций и иных сделок, и другой необходимой информации.

2.2.3. При обращении физического лица – клиента с заявлением в Банк для открытия сберегательного счета ответственный сотрудник Отдела розничных услуг, при обращении для получения банковской пластиковой карточки или осуществления через расположенный в Банке терминал операций (снятие наличных средств, оплата товаров и услуг) с использованием пластиковой карты, за исключением оплаты коммунальных услуг, услуг связи, платежей в бюджет, внебюджетные фонды и других обязательных платежей, – ответственный сотрудник Отдела розничных услуг, при обращении за получением кредита – ответственный сотрудник Отдела кредитных операций, при обращении по разовым операциям, проводимым через кассу Банка, если для осуществления данной разовой операции требуется идентификация клиента на основании настоящих Правил, – ответственный сотрудник Отдела кассовых операций, на которого возложена соответствующая функция, идентифицирует клиента.

Начальник Отдела кассовых операций несет ответственность за обеспечение идентификации клиента по разовой операции, осуществляемой им через кассу Банка, и заполнение его электронной анкеты.

2.2.4. При обращении физического лица – клиента с заявлением в центре банковских услуг для открытия сберегательного счета, при обращении для получения банковской пластиковой карточки или осуществления через расположенный в Банке терминал операций (снятие наличных средств, оплата товаров и услуг) с использованием пластиковой карты, за исключением оплаты коммунальных услуг, услуг связи, платежей в бюджет, внебюджетные фонды и других обязательных платежей, ответственный сотрудник центра банковского услуги идентифицирует клиента.

2.2.5. При обращении клиента в Банк для осуществления разовой операции, если для осуществления данной разовой операции требуется идентификация клиента на основании настоящих Правил, ответственный сотрудник для идентификации клиента после ознакомления с оригиналом документа, подтверждающим его личность, проверяет наличие электронной анкеты клиента в АБС. В случае отсутствия электронной анкеты клиента, ответственный сотрудник берет копию документа, подтверждающую его личность, и на основании полученных идентификационных сведений формирует электронную анкету клиента, с указанием даты осуществления операции и вида операции.

А при наличии электронной анкеты клиента, ответственный сотрудник проверяет соответствие сведений в документе, подтверждающем его личность, со сведениями в электронной анкете. При полном совпадении сведений, не требуется получение копии документа, подтверждающего личность клиента. А при несовпадении сведений по некоторым причинам (документ обновлен, изменен адрес и т.п.), ответственный сотрудник берет копию документа, подтверждающего личность, и вносит соответствующие изменения в электронную анкету клиента.

2.2.6. Сведения, полученные в результате надлежащей проверки клиентов осуществивших разовые операции, обновляются при осуществлении последующих операций, требующих принятия надлежащей проверки клиента.

2.3. Идентификация индивидуальных предпринимателей, а также юридических лиц и их реальных владельцев

2.3.1. Идентификация индивидуального предпринимателя, юридического лица и его реального клиента в Банке осуществляется на основе информации, предусмотренной приложениями № 2 к настоящим Правилам, а также документов, являющихся основанием совершения операций и иных сделок, и другой необходимой информации.

2.3.2. При выполнении мер надлежащей проверки клиентов в отношении клиентов - юридических лиц и индивидуальных предпринимателей, Отдел по корпоративному обслуживанию юридических лиц должен получить от них соответствующие документы о государственной регистрации, сведения о руководителях, а также сведения, указанные в учредительных документах.

Получение указанных сведений осуществляется через автоматизированную систему государственной регистрации и постановки на учет субъектов предпринимательства либо непосредственно от клиента в случае, когда получение информации из данной системы невозможно.

В процессе надлежащей проверки юридических лиц Отдел по корпоративному обслуживанию юридических лиц должен предпринять обоснованные и доступные меры по идентификации физического лица - бенефициарного собственника клиента, которое в конечном итоге является собственником или контролирует клиента, в том числе путем изучения структуры собственности и управления клиента, а также учредителей (акционеров, участников) клиента.

структуры собственности и управления клиента;

учредителей клиента (акционеров/участников, являющихся владельцами не менее десяти процентов акций/долей общества);

личных данных физического лица (лиц), владеющего в конечном итоге долей (не менее десяти процентов) юридического лица (если такие имеются);

если возникают сомнения в результате принятых мер в отношении того, является ли лицо (лица), имеющее контрольную долю, бенефициарным собственником или в случае отсутствия лиц, осуществляющих управление правом собственности долей, личных данных физического лица (лиц), осуществляющего контроль над юридическим лицом другими методами (если такие имеются).

При невозможности выявления бенефициарного собственника соответствующими мерами, принятыми коммерческими банками, банк должен идентифицировать лицо, занимающее высокую руководящую должность, и принять обоснованные меры по проверке его личности.

2.3.3. Если клиентом или бенефициарным собственником клиента является юридическое лицо, на которое распространяются требования нормативно-правовых актов о раскрытии информации о структуре собственности, то установление и подтверждение личности учредителей (акционеров, являющихся владельцами не менее чем десяти процентов акций общества, участников) такого юридического лица не требуются.

2.3.4. К иностранным структурам без образования юридического лица применяются требования, установленные настоящих Правилах к юридическим лицам.

2.3.5. В целях более тщательного изучения клиента - юридического лица необходимо уделять особое внимание:

составу учредителей (акционеров, участников) клиента, определению лиц, владеющих долей свыше 10 процентов уставного фонда (капитала) клиента;

структуре органов управления клиента и их полномочиям;

размеру зарегистрированного уставного фонда (капитала) клиента.

2.3.6. При обращении юридического лица или индивидуального предпринимателя – клиента в Банк за получением кредита, ответственный сотрудник Отдела кредитных операций должен осуществить его надлежащую проверку и сверить идентификационные сведения с данными в анкете. Если данные в электронной анкете клиента расходятся с представленными клиентом сведениями, ответственный сотрудник Отдела кредитных

операций сообщает об этом начальнику Отдела по обслуживанию клиентов и сотруднику Службы внутреннего контроля.

2.3.7. Сведения, полученные в результате надлежащей проверки клиентов, должны обновляться не реже одного раза в год в случаях, когда Банк оценивает риск осуществления клиентом легализации доходов, полученных от преступной деятельности, финансирования терроризма и финансирования распространения оружия массового уничтожения, как высокий, в иных случаях не реже одного раза в два года и при наличии изменений в сведениях клиента.

Для обновления имеющихся в Банке идентификационных сведений клиента начальник Отдела по корпоративному обслуживанию юридических лиц до конца месяца составляет список клиентов, которым присвоен высокий уровень риска с даты последней идентификации один год и два года для остальных клиентов и распределяет их ответственным сотрудникам.

Ответственные сотрудники в течение одного месяца принимают меры по изучению и обновлению реальных идентификационных сведений клиентов, указанных в данном списке.

2.3.8. При внесении изменений в имеющиеся идентификационные сведения клиента, соответствующий сотрудник Отдела по корпоративному обслуживанию юридических лиц должен внести надлежащие изменения в анкету клиента и сообщить об этом сотруднику Службы внутреннего контроля.

2.3.9. Начальник Отдела по корпоративному обслуживанию юридических лиц несет ответственность за своевременное и правильное выполнение обязанностей по надлежащей проверке юридических лиц и индивидуальных предпринимателей – клиентов и заполнению их электронных анкет.

2.4. Осуществление углубленного мониторинга установления деловых отношений с публичными должностными лицами и их близкими родственниками, а также проводимых ими операций

2.4.1. Помимо применения вышеуказанных мер по надлежащей проверке клиента, в отношении публичных должностных лиц, выступающих в качестве клиента или бенефициарного собственника клиента, сотрудники Банка должны:

применять разумные меры для проверки сведений о статусе публичного должностного лица и определения источника денежных средств или иного имущества по операции;

устанавливать (или продолжать для существующих клиентов) деловые отношения с публичным должностным лицом только с разрешения председателя правления банка или его уполномоченного заместителя;

осуществлять постоянный углубленный мониторинг деловых отношений.

2.4.2. В ходе надлежащей проверки клиента ответственный сотрудник подразделения по работе с клиентами должен принять разумные и доступные меры для проверки клиента и лиц, действующих от имени клиента, бенефициарного собственника клиента на принадлежность к публичным должностным лицам. При этом, проверка клиента и лиц, действующих от имени клиента, а также бенефициарного собственника клиента на принадлежность к публичным должностным производится до установления деловых отношений с клиентом, на основе сведений полученных при идентификации.

Для этого ответственный сотрудник, если клиент и лица, выступающие в качестве клиента, бенефициарного собственника клиента не являются гражданами Республики Узбекистан, или являются юридическими лицами, зарегистрированными в других государствах, должен обратить внимание на их наименование, получить дополнительные подтвержденные сведения из открытых источников и баз данных, в случае необходимости, обратиться к сотруднику Службы внутреннего контроля филиала для получения дополнительной информации.

Если будет установлено, что клиента и лица, выступающие в качестве клиента, бенефициарного собственника клиента являются публичными должностными лицами, ответственный сотрудник соответствующего отдела до установления отношений с клиентом и или осуществления его операций, должен незамедлительно письменно сообщить о таком клиенте управляющему филиала и сотруднику Службы внутреннего контроля филиала. В свою очередь руководитель филиала должен письменно сообщить о публичном должностном лице председателю правления или его уполномоченному заместителю, а также попросить соответствующие указания по вступлению с ним в отношения.

2.4.3. Сотрудник Службы внутреннего контроля филиала после получения сообщения ответственного сотрудника о выявлении публичного должностного лица, должен сообщить об этом руководителю Службы внутреннего контроля. Служба внутреннего контроля после получения сообщения о том, что клиент и лица, выступающие в качестве клиента, бенефициарного собственника клиента являются публичными должностными лицами, должна предпринять следующие меры:

по мере возможности подробно идентифицировать личность клиента и бенефициарного собственника клиента, а также получить дополнительные сведения о клиенте из открытых баз данных или через базовые программы специальных лиц;

принять меры по выявлению источника денежных средств клиента или его финансового положения, в том числе через получение информации от клиента;

присвоить клиенту высокий уровень риска;

оценить риск установления отношений с клиентом и осуществления его операций;

сообщить о выявленном публичном должностном лице председателю правления или его уполномоченному заместителю;

рассмотреть вопрос сообщения в Департамент об операции публичного должностного лица;

усилить мониторинг за операциями клиента.

2.4.4. Председатель правления или его уполномоченный заместитель не позднее дня поступления сообщения должен дать соответствующее указание об установлении или не установлении отношений с публичным должностным лицом.

Соответствующее указание незамедлительно доводится в установленном порядке до руководителя филиала и ответственных сотрудников. Если в указании сказано о необходимости установлении отношений с клиентом, руководитель филиала и ответственные сотрудники устанавливают отношения с клиентом. Применяются усиленные меры по надлежащей проверке клиентов в отношении публичных должностных лиц.

2.4.5. Сотрудники Службы внутреннего контроля филиала в качестве дополнительной меры выявления публичных должностных лиц, если клиент и лица, выступающие в качестве клиента, бенефициарного собственника клиента не являются гражданами Республики Узбекистан, или являются юридическими лицами, зарегистрированными в других государствах, должны обратить внимание на их наименование, получить дополнительные подтвержденные сведения о клиенте из открытых источников и баз данных, а также контролировать осуществление в установленном порядке выявления публичных должностных лиц ответственными сотрудниками.

2.5. Надлежащая проверка банков-нерезидентов при установлении и осуществлении корреспондентских отношений

2.5.1. При установлении и осуществлении корреспондентских отношений с банком-нерезидентом идентификация банка-нерезидента осуществляется Управлением внешнеэкономической деятельности.

2.5.2. При идентификации Управлению внешнеэкономической деятельности необходимо:

В банке, выступающие в качестве транзитного финансового учреждения, в случаях, когда технические ограничения препятствуют сохранению привязанной к внутреннему электронному переводу требуемой информации об отправителе и получателе, сопровождающей международный электронный перевод, должны хранить запись всей информации, полученной от отправлявшего финансового учреждения или другого транзитного финансового учреждения, не менее пяти лет.

собрать информацию о банке-нерезиденте для того, чтобы получить полное представление о характере его деловой деятельности;

определить на основе открытой информации репутацию и качество надзора, в том числе проводились ли в отношении этого банка расследования нарушений, связанных с легализацией доходов, полученных от преступной деятельности, финансированием терроризма и финансированием распространения оружия массового уничтожения или применялись ли в отношении него меры со стороны контролирующих органов;

оценивать применяемые банком-нерезидентом меры по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения;

в отношении «транзитных счетов» — получать соответствующее подтверждение об исполнении банком-респондентом обязанности по проведению надлежащей проверки в отношении своих клиентов, имеющих прямой доступ к счетам банка-корреспондента, а также о возможности предоставления по запросу банка-корреспондента необходимых данных о клиенте, полученных в результате идентификации;

Решение об установлении корреспондентских отношений с банком-нерезидентом принимается Правлением Банка.

2.5.3. Управление внешнеэкономической деятельности должно направить банку-нерезиденту, с которым устанавливаются корреспондентские отношения, запросы о наличии возможности предоставления необходимых сведений касающихся необходимой идентификации для осуществления работ по противодействию легализации доходов, полученных от преступной деятельности, и финансирования терроризма, и принять необходимые меры для получения подтверждения.

2.5.4. Управление внешнеэкономической деятельности должно направить зарубежному банку, с которым устанавливаются корреспондентские отношения, анкету по форме указанной в приложении № 4 к настоящим Правилам, если он зарегистрирован на территории государств СНГ, и по форме указанной в приложении № 5 к настоящим Правилам, если он зарегистрирован на территории других государств, и принять необходимые меры для его возврата с подтверждением.

Управление внешнеэкономической деятельности предоставляет Службе внутреннего контроля цветную отсканированную копию подтверждения и анкеты, полученных из зарубежного банка-нерезидента.

2.5.5. Банку необходимо убедиться в том, что банки-нерезиденты, с которыми устанавливаются корреспондентские отношения, применяют международные стандарты проверки и используют соответствующие процедуры проверки к операциям.

2.5.6. Решение об установлении корреспондентских отношений с банком-нерезидентом принимается Правлением Банка.

2.5.7. Соответствующие подразделения Банка при установлении отношений с другими банками с целью осуществления транзитных переводов должны сохранять всю информацию об электронных платежах.

2.5.8. Обеспечение четкого и полного распределения обязанностей между корреспондентами Управление внешнеэкономической деятельности.

2.5.9. Управление внешнеэкономической деятельности должно принять меры по отражению в заключаемых с банками-корреспондентами нерезидентами договорах соответствующих пунктов, чтобы иметь возможность в течение трех рабочих дней получить дополнительные сведения об отправителях денежных средств.

При отсутствии такой возможности, Банк должен рассмотреть вопрос по прекращению договора с такими банками-корреспондентами нерезидентами.

2.5.10. При продолжении корреспондентских отношений с банками-нерезидентами, расположенными на территории государств, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, или их дочерними банками, филиалами и представительствами, соответствующие подразделения Банка, а также Служба внутреннего контроля должны проявлять особое внимание всем осуществляемым с ними операциям.

Банк:

обязан предпринимать меры, направленные на предотвращение установления отношений с банками-нерезидентами, в отношении которых имеется информация о том, что их счета используются банками, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления;

может при проведении международных расчетов обмениваться с банками-корреспондентами деталями платежа и другой информацией, связанной с осуществлением вышеуказанных расчетов;

должен уделять особое внимание и проводить тщательный анализ операций, связанных с международными денежными переводами, в которых сведения об отправителе (фамилия, имя, отчество физических лиц, полное наименование юридических лиц, местонахождение (почтовый адрес) и номер счета отправителя) не представлены либо представлены не в полном объеме.

должны усилить контроль за деятельностью их зарубежных дочерних банков, филиалов и представительств, находящихся в государствах, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;

обязаны требовать от своих зарубежных дочерних банков, филиалов и представительств информировать головной офис, в случае невозможности применения соответствующих мер по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения из-за имеющегося запрета актами законодательства страны, в которой находятся дочерние банки, филиалы и представительства. В свою очередь, Банк уведомляет об этом Центральный банк и Департамент и принимает соответствующие дополнительные меры по управлению рисками, связанными с легализацией доходов, полученных от преступной деятельности, финансированием терроризма и (или) финансированием распространения оружия массового уничтожения.

2.5.11. В случае наличия информации о случаях нарушения банком-нерезидентом требований международных стандартов по противодействию легализации доходов, полученных от преступной деятельности, и финансирования терроризма, Правление Банка должно рассмотреть вопрос о принятии соответствующих мер вплоть до прекращения сотрудничества с данным корреспондентом.

2.5.12. Настоящие правила обязательные для исполнения платежными агентами Банка и их платежными субагентами, а также всеми подразделениями и дочерними банками филиалами и представительствами Банка за рубежом.

2.5.13. При заключении агентского договора с платежным агентом Управление вкладных и транзакционных операций Банка ответственно за включение требования о соблюдении настоящих Правил в агентский договор, а также за контроль включения данного требования в субагентские договора, заключаемые между платежным агентом и платежным субагентом. Управление вкладных и транзакционных операций контролирует доведение в бумажном или электронном виде копии настоящих правил до платежного агента Банка.

2.6. Надлежащая проверка компаний, предоставляющих услуги по международным денежным переводам через системы международных денежных переводов и международные системы пластиковых карт, при установлении и осуществлении с ними отношений

2.6.1. Идентификация компаний, оказывающих услуги по системе международных денежных переводов (далее по тексту - системы международных денежных переводов), и компаний, оказывающих услуги по системе платежей через международные пластиковые карты (далее по тексту – международные системы пластиковых карт), при установлении с ними отношений осуществляется Управление вкладных и транзакционных операций и Управление карточного бизнеса.

2.6.2. Управление вкладных и транзакционных операций, помимо идентификации, должен:

собрать информацию о партнере по международным денежным переводам и международным пластиковым картам для того, чтобы получить полное представление о характере его деловой деятельности;

определить на основе открытой информации репутацию, в том числе проводились ли в отношении этой организации расследования нарушений, связанных с легализацией доходов, полученных от преступной деятельности, и финансированием терроризма;

сохранять всю информацию об электронном переводе.

2.6.3. Решение об установлении отношений с системами международных денежных переводов и международными системами пластиковых карт, принимается Правлением Банка.

2.6.4. Управление вкладных и транзакционных операций принимает необходимые меры к системам международных денежных переводов и системам международных пластиковых карт при установлении отношений с последующим направлением не реже одного раза в два года анкеты по форме, указанной в приложении № 4 к настоящим Правилам, если он зарегистрирован на территории государств СНГ, и анкеты по форме, указанной в приложении № 5 к настоящим Правилам, если он зарегистрирован на территории других государств, с ее заполнением и подтверждением.

2.6.5. Управление вкладных и транзакционных операций и Управление карточного бизнеса предоставляет Службе внутреннего контроля цветную отсканированную копию анкеты, полученной из системы международных денежных переводов и международной системы пластиковых карт. Служба внутреннего контроля может также запросить другие сведения по изучению данной системы.

2.6.6. При осуществлении операций по денежным переводам, а также операций через международные системы денежных переводов, Управление вкладных и транзакционных операций должно вести учет подразделений (филиалов, отделов и т.п.) Банка, осуществляющих такие услуги и сотрудников этих подразделений.

2.6.7. Управление вкладных и транзакционных операций совместно с подразделениями, оказывающими услуги по осуществлению международных денежных переводов, должно:

обеспечить сопровождения отправляемых денежных переводов точными сведениями о клиенте-отправителе (наименование отправителя; серия и номер документа (паспорта или заменяющего его документа), удостоверяющего личность — для физических лиц; номер счета, если в процессе операции использовался счет клиента или уникальный код операции; адрес отправителя или государственный идентификационный номер либо идентификационный номер клиента или для физических лиц дата и место рождения), и о получателе (наименование получателя; номер счета, если в процессе операции использовался счет клиента или уникальный номер операции);

требовать от банков-нерезидентов и систем международных денежных переводов предоставления минимальной информации (наименование отправителя); номер счета, если в процессе операции использовался счет клиента или уникальный номер операции)

об отправителях денежных средств, сумма которых не достигает 50-кратный размер базовой расчетной величины;

требовать от банков-нерезидентов и систем международных денежных переводов предоставления минимальной информации (наименование отправителя; серия и номер документа (паспорта или заменяющего его документа), удостоверяющего личность — для физических лиц; адрес отправителя или государственный идентификационный номер либо идентификационный номер отправителя или для физических лиц дата и место рождения; номер счета отправителя, если в процессе операции использовался счет клиента или уникальный номер операции) об отправителях денежных средств, сумма которых равна или превышает 50-кратный размер базовой расчетной величины;

принимать обоснованные и доступные меры по выявлению международных денежных переводов, не имеющих требуемой информации о получателе и (или) отправителе.

Электронные денежные переводы, не содержащие требуемой информации о получателе или отправителе, будут отклонены ответственным сотрудником. В случае получения дополнительной информации о получателе и отправителе через клиентские или международные системы денежных переводов, эти денежные переводы должны будут осуществить ответственные сотрудники. О таких переводах ответственное лицо должно уведомить сотрудников службы внутреннего контроля. Сотрудник службы внутреннего контроля должен будет пересмотреть уровень риска для данной операции или клиента и сообщить об этом в Департамент.

запрещается оказывать услуги по переводу денежных средств, в том числе через системы международных денежных переводов, если денежный перевод не соответствуют требованиям, установленным настоящим пунктом.

2.6.8. Данные об отправляемых внутренних электронных денежных переводах, сумма которых равна или превышает 36-кратный размер базовой расчетной величины должны включать в себя сведения об отправителе, полученные в ходе идентификации клиента и сведения о получателе, в соответствии с пунктом 2.6.7, кроме случаев, когда полная информация об отправителе может быть получена с помощью других источников. В таких случаях Управление вкладных и транзакционных операций включает персональный идентификационный номер физического лица, а также номер счета или уникальный код операции (идентификатор) при условии, что этот номер счета или идентификатор позволит проследить операцию назад до отправителя или получателя.

Управление вкладных и транзакционных операций должно обеспечить сопровождение внутренних электронных денежных переводов, сумма которых не достигает 36-кратный размер базовой расчетной величины, информацией об отправителе (наименования отправителя; номер счета отправителя, когда в процессе операции использовался такой счет или уникальный код операции) и о получателе (наименования получателя; номер счета получателя, когда в процессе операции использовался такой счет или уникальный код операции).

2.6.9. Информация о внутренних электронных денежных переводах должна включать информацию об отправителе, как и в случае международных денежных переводов.

Управление вкладных и транзакционных операций должно принять меры по отражению в заключаемых с системами международных денежных переводов договорах соответствующих пунктов, чтобы иметь возможность в течение трех рабочих дней получить дополнительные сведения об отправителях денежных средств.

При отсутствии такой возможности, Банк должен рассмотреть вопрос о прекращении договора с такими системами международных денежных переводов.

2.6.10. В случае, если банк оказывает услуги как отправляющей, так и принимающей сторонам по переводам денежных средств, на Службу внутреннего контроля возлагаются следующие обязанности:

принять во внимание всю информацию, полученную как от отправляющей стороны,

так и от получающей стороны, для определения необходимости направления сообщения о подозрительной операции;

направить сообщение о подозрительной операции в компетентные органы в любой стране, с которой связан подозрительный денежный перевод, и предоставить соответствующую информацию о денежном переводе.

III.ПРАВИЛА ОСУЩЕСТВЛЕНИЯ МОНИТОРИНГА ЗА ОПЕРАЦИЯМИ

3.1. Критерии и признаки сомнительных и подозрительных операций

3.1.1. Операция признается сомнительной при наличии одного из нижеследующих критериев и признаков:

1) операции или клиенту, ее осуществляющему, Банком присвоен высокий уровень риска;

2) систематически осуществляемый возврат клиентом-резидентом ранее полученной суммы в пользу нерезидента по договору поставки товаров (выполнения работ, оказания услуг);

3) предоставленные документы на проведение операции вызывают сомнение в их подлинности (достоверности), и (или) сведения об операции, в том числе о какой-либо из ее сторон, не соответствуют имеющейся у Банка информации;

4) необычность в поведении клиента при обращении с заявлением (поручением, ходатайством) о совершении операции, например: нервозность, неуверенность, агрессия с одновременным присутствием лиц, руководящих действиями клиента, либо его обращением по телефону к другим лицам за советом по незначительному поводу;

5) необычная озабоченность клиента вопросами конфиденциальности или необоснованный отказ либо неоправданные задержки в представлении клиентом информации об операции, запрашиваемой сотрудниками Банка;

6) невозможность установления партнеров клиента по проводимой операции;

7) операция не имеет явного экономического смысла и не соответствует характеру и виду деятельности клиента;

8) необоснованное увеличение оборота денежных средств по счету клиента, не связанное с характером его деятельности и (или) произошедшее после более, чем трехмесячного периода низкой активности либо отсутствия признаков активности на счетах данного клиента;

9) необоснованное и (или) досрочное прекращение деловых отношений по инициативе клиента, сопровождаемое снятием или переводом всех средств в другие коммерческие банки;

10) немедленное прекращение деловых отношений по инициативе клиента после обоснованного применения коммерческим банком мер, предусмотренных настоящими Правилами;

11) явное несоответствие операций, проводимых клиентом с участием Банка, общепринятой практике совершения операций;

12) необоснованное дробление сумм аналогичных операций, совершаемых клиентом на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины на день осуществления операции;

13) порядок проведения расчетов содержит нестандартные или необычно сложные схемы, отличающиеся от обычной деятельности клиента;

14) обмен банкнот одного достоинства на банкноты другого достоинства физическим лицом на сумму, равную или превышающую 500-кратный размер минимальной заработной платы, установленный на день обмена;

15) внесение физическим лицом в наличной форме денежных средств на сумму, равную или превышающую 500-кратный размер базовой расчетной величины на день осуществления операции, на банковский счет юридического лица или индивидуального предпринимателя в качестве займов, финансовой помощи, вклада в уставный фонд

(капитал) либо оборотных средств в целях пополнения;

16) перечисление со счетов юридических лиц или индивидуальных предпринимателей денежных средств на сумму, равную или превышающую 1000-кратный размер базовой расчетной величины на день осуществления операции, в качестве финансовой помощи или займа; перечисление со счетов юридических лиц или индивидуальных предпринимателей денежных средств на сумму, равную или превышающую 500-кратный размер минимальной заработной платы на день осуществления операции, в качестве финансовой помощи или займа;

17) перечисление со счетов юридических лиц и/или индивидуальных предпринимателей в пользу физических лиц денежных средств на сумму, равную или превышающую 1000-кратный размер базовой расчётной величины на день осуществления операции, в качестве дивидендов или прибыли;

18) снятие со счета физического лица денежных средств в наличной форме на сумму, равную или превышающую 500-кратный размер базовой расчетной величины на день осуществления операции;

19) осуществление операций (оплата или снятие наличности) с пяти и более международных платежных карт в течение одного дня по терминалу одного контрагента, когда сумма операций с каждой картой равна или превышает 25-кратный размер базовой расчётной величины.;

20) перечисление денежных средств, сумма которых равна или превышает 500-кратный размер базовой расчётной величины, за пределы Республики Узбекистан на счет получателя, открытый в банке, местонахождение которого отличается от места регистрации получателя.

21) перечисление физическим лицом на имя другого физического лица денежных средств, сумма которых равна или превышает 1000- кратный размер базовой расчётной величины на день осуществления операции.

22) осуществление платежей сумму, равную или превышающую 1000- кратный размер базовой расчётной величины установленную на дату сделки с пластиковых карт, эмитированных Банком или с пластиковых карт, эмитированных другим банком через терминал, установленный Банком.

3.1.2. Операция признается подозрительной при наличии одного из нижеследующих критериев и признаков:

1) одной из сторон операции является лицо, постоянно проживающее, находящееся или зарегистрированное в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;

2) получение отправленных из-за рубежа или отправление за рубеж физическими лицами (в том числе несколькими физическими лицами на имя одного контрагента) денежных средств в иностранной валюте, в том числе через системы денежных переводов, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины, единовременно или многократно в течение срока, не превышающего 1 месяца;

3) продажа или покупка, а также снятие с международных платежных карт физическими лицами и/или индивидуальными предпринимателями денежных средств в иностранной валюте на сумму, равную или превышающую 500-кратный размер базовой расчетной величины, единовременно или многократно в течение срока, не превышающего 1 месяца;

4) перечисление денежных средств за пределы Республики Узбекистан на счет, открытый на анонимного владельца, и поступление денежных средств в Республику Узбекистан со счета, открытого на анонимного владельца или при отсутствии сведений об отправителе;

5) перечисление денежных средств за пределы Республики Узбекистан на счет получателя, открытого в банке, зарегистрированном в оффшорной зоне, отличающейся от места регистрации получателя;

6) денежные средства переводятся за пределы Республики Узбекистан на счета или в пользу лиц, постоянно проживающих или зарегистрированных в оффшорных зонах, либо поступают в Республику Узбекистан со счетов таких лиц единовременно или многократно в течение 30 дней, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины, установленный на день последнего перевода (поступления);

7) операции с клиентами-нерезидентами, информация об учредителях которых отсутствует и получить ее всеми доступными методами невозможно;

8) операция, связанная с использованием денежных средств или иного имущества, к которым предоставлен доступ, включая попытку ее проведения;

9) другие операции, не имеющие критериев и признаков, предусмотренных в данном пункте, установленных настоящими Правилами, в отношении которых у коммерческого банка имеются подозрения в причастности к легализации доходов, полученных от преступной деятельности, и (или) финансированию терроризма.

10) передача нерезидентом резиденту денежных средств в качестве грантов, финансовой помощи, займов или безвозмездной помощи;

11) отправка и получение денежных средств через системы международных денежных переводов гражданами Республики Узбекистан, находящиеся в зонах с повышенной террористической активностью (список стран и территории предоставляется Департаментом);

12) операции лиц, которые находятся в межгосударственном розыске за совершение преступлении террористического характера (перечень лиц предоставляется Департаментом);

13) денежный оборот юридического лица — клиента равен или превышает 20000-кратный размер базовой расчетной величины в течение срока, не превышающего 3 месяцев с момента создания данного юридического лица, и осуществляется с целями, не соответствующими характеру его деятельности;

14) покупка физическими лицами монет, мерных слитков Центрального банка из драгоценных металлов на сумму, равную или превышающую 500-кратный размер базовой расчетной величины, единовременно или многократно в течение срока, не превышающего 1 месяца.

15) Подозрительные операции, решение о включении которых в категорию операций подлежит сообщению Службой внутреннего контроля.

3.2. Выявление сомнительных и подозрительных операций

3.2.1. Изучение деятельности клиентов осуществляется систематической проверкой и контролированием их операций.

Проверка операций клиентов состоит из текущей и последующей проверки.

Текущая проверка операций клиента в Банке и его филиалах осуществляется подразделениями, осуществляющими и контролирующими его операции в следующих этапах, указанных в разделе III «Инструкции о порядке организации ведения бухгалтерского учета и бухгалтерских работ в банках Республики Узбекистан» (зарегистрированной 11 июля 2008 года в Министерстве юстиции за № 1834):

а) первичный контроль;

б) текущий контроль;

в) заключительный контроль.

Осуществление операций в подразделениях Банка должно быть организовано на основании данного принципа трехэтапного контроля. На каждом этапе контроля соответствующие сотрудники, наряду с контролированием правильного оформления

документа, должны обратить внимание на суть операции, ее связанность или не связанность с видом деятельности клиента.

3.2.2. Информация, полученная в ходе идентификации, а также присвоенный уровень риска работы с клиентом являются основой для мониторинга операций, осуществляемых (осуществленных) клиентами, проводимого для того, чтобы убедиться о соответствии таких операций основным направлениям деятельности клиента, и изучения при необходимости источников средств.

3.2.3. Текущая проверка операций клиентов проводится соответствующими сотрудниками Банка, непосредственно обслуживающими клиентов (ответственными исполнителями, кассирами, специалистами по пластиковым картам, кредитованию и т. п.), которые при выявлении операций, имеющих признаки подозрительных и (или) сомнительных операций, обязаны незамедлительно в письменном виде сообщить о таких операциях своему непосредственному руководителю и сотрудникам Службы внутреннего контроля, с указанием соответствующих критериев и признаков указанных в приложении № 7 к настоящим Правилам. При осуществлении физическими лицами подозрительных операций, вместе с сообщением об операции предоставляется копия документа, послужившего основанием для осуществления операции.

При отсутствии возможности выражения деталей сомнительной операции по форме, указанной в приложении № 7 к настоящим правилам, непосредственно обслуживающие клиентов ответственные сотрудники могут передать сообщение по сомнительной операции в удобной для себя форме. Кроме этого, можно передать одним сообщением по идентичным операциям (например, осуществляемые с терминала клиента операции и т.п.) или в форме таблицы, с приложением к сообщению.

Последующая проверка операций клиентов проводится сотрудниками Службы внутреннего контроля филиала посредством анализа совершенных за предыдущий период операций клиента с целью выявления сомнительных и подозрительных операций, не определяемых на стадии текущей проверки.

3.2.4. При выявлении операций, имеющих признаки сомнительных и (или) подозрительных операций, сотрудники коммерческого банка, непосредственно обслуживающие клиентов, по поручению Службы внутреннего контроля при необходимости обращаются к клиенту за дополнительными сведениями о проводимой операции.

3.2.5. Общение с клиентами осуществляется сотрудниками подразделения, непосредственно обслуживающими клиентов. Также и ответственные сотрудники Службы внутреннего контроля могут получить дополнительные сведения необходимые для надлежащего изучения клиента через сотрудников, непосредственно обслуживающих клиентов.

3.2.6. Сотрудники Службы внутреннего контроля изучают сведения о клиенте и операции, заносят соответствующую информацию в специальный журнал Службы внутреннего контроля по форме, приведенной в приложении № 8, в файл «Messages» в виде защищенной паролем электронной таблицы по форме, приведенной в приложении № 14, и в анкету клиента, а также при наличии достаточных оснований, направляют руководителю Службы внутреннего контроля предложение о классификации сомнительной операции как подозрительной. 3

3.2.7. Уведомления о подозрительных операциях, предоставляемые ответственными сотрудниками, регистрируются в хронологическом порядке в специальной электронной папке «Сообщения» сотрудниками службы внутреннего контроля филиала и ежедневно направляются в Головной офис в Управление комплаенс-контроля по почте «Lotus Notes» с защищенным паролем. ".

Сотрудник Управление комплаенс-контроля головного банка ежедневно собирает данные о подозрительных операциях со всех филиалов в единый электронный файл «Сообщения-9055» и проводит анализ подозрительных операций с начальником Управление комплаенс-контроля.

3.2.8. В случае возникновения обоснованных подозрений руководитель Службы внутреннего контроля принимает письменное решение о признании операции клиента подозрительной и информирует об этом руководство банка.

В отдельных случаях, исходя из уровня риска сомнительных операций, может быть разрешено немедленное отнесение их к подозрительным на основании письменного указания (распоряжения) руководства Банка.

3.2.9. Признание операций подозрительными осуществляется на основе комплексного анализа с использованием критериев и признаков подозрительных операций, определяемых настоящими Правилами в каждом отдельном случае

3.2.10. Признание операций подозрительной в каждом случае основывается на комплексном анализе с использованием критериев и признаков подозрительных операций, установленных настоящими Правилами.

После признания операции клиента подозрительной Служба внутреннего контроля должна принять нижеследующие меры:

предоставить сообщение о подозрительной операции в Департамент;

получить дополнительную информацию о клиенте;

пересмотреть уровень риска клиента;

усилить мониторинг за операциями клиента;

внести предложение председателю правления коммерческого банка о прекращении договорных отношений с клиентом в соответствии с законодательством и заключенным с ним договором.

3.2.11. Сообщение о подозрительной операции передается Службой внутреннего контроля в Департамент не позднее одного рабочего дня, с момента выявления подозрительной операции, в соответствии с требованиями Приложения 1 «Положение о порядке предоставления информации, связанной с противодействием легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения» утвержденного постановлением Кабинета Министров Республики Узбекистан № 402 от 29 июня 2021 года.

3.3.Подготовка сообщений о подозрительных операциях и их направление в Департамент

3.3.1. При выявлении операций соответствующих критериям и признакам подозрительности, предусмотренным в подпунктах 1-9 пункта 3.1.2 к настоящим правилам, сообщения по ним не позднее дня, в котором они были выявлены, сотрудниками службы внутреннего контроля филиала направляются в Головной офис по почте «Lotus Notes» в виде сформированного файла с применением криптографической защиты с помощью специальной программы, а также в виде защищенной паролем электронной таблицы, приведенной в приложении № 14. Службой внутреннего контроля в Головном банке сообщения по таким подозрительным операциям представляются в Департамент не позднее следующего рабочего дня, без привязки их анализа.

3.3.2. При выявлении операций соответствующих критериям и признакам сомнительности, предусмотренным в пункте 4.1.1 к настоящим правилам, сообщения по ним сотрудниками службы внутреннего контроля филиала направляются в Головной банк по почте «Lotus Notes» в виде защищенной паролем электронной таблицы, приведенной в приложении № 14.

Поступившие с филиалов сомнительные операции собираются и анализируются, перечень операций, признанных из них подозрительными, направляется в каждый филиал по почте «Lotus Notes» в виде защищенной паролем электронной таблицы. Сотрудники службы внутреннего контроля филиала не позднее дня получения перечня направляют сведения о подозрительных операциях в Головной банк по почте «Lotus Notes» в виде сформированного файла с применением криптографической защиты с помощью

специальной программы, а также в виде защищенной паролем электронной таблицы, приведенной в приложении № 14.

3.3.3. Заполненные сотрудниками службы внутреннего контроля филиала сведения по подозрительным операциям формируются в комплексе автоматизированных программных средств по внесению, обработке и передаче информации «Moneyoper». В сведение данные и реквизиты должны быть внимательно и правильно внесены. Отправленные в Головной банк файлы с электронными сообщениями должны храниться в отдельной папке.

Файлы, принятые из филиалов сотрудником службы внутреннего контроля филиала, хранятся отдельно по каждому филиалу в открытой для сообщений папке «Messages/Incoming». Данные поступившие файлы открываются с помощью программы «Moneyoper», проверяются и исправляются при наличии ошибок и недостатков. Затем сообщения повторно сохраняются в папке «Messages/Incoming» в виде электронного документа, с применением криптографической защиты и применением средств электронной передачи, подтверждаются электронной цифровой подписью в законодательном порядке и отправляются в Департамент через специальную защищенную связь с помощью почты «Lotus Notes».

3.3.4. При отсутствии отправки в Департемент сообщений в форме электронного документы через специальную защищенную связь, они отправляются в Департамент через носители электронной информации (дискета, компакт-диск и другие установки памяти), доставляются нарочно или посредством специальной почтовой связи с исключением случаев угрозы конфиденциальности документа.

3.3.5. В случае отсутствия возможности отправки сообщений в форме электронного документа, они предоставляются нарочно или с помощью специальной целевой почтовой связи на бумажном носителе, с соблюдением требований порядка исключающего нарушение конфиденциальности документа.

При предоставлении сообщений нарочно или через специальную почту, датой их предоставления считается дата их вручения нарочно или передача в установленном порядке в специальную почту.

3.3.6. Информация о каждом сообщении заносится в специальный журнал.

Служба внутреннего контроля ежедневно формирует в бумажных носителях в виде таблицы информацию о переданных сообщениях в Департамент, с указанием всех сведений из электронного сообщения. Данная таблица должна визироваться исполнителем и утверждаться руководителем Службы внутреннего контроля.

При формировании таких таблиц не требуется переносить электронное сообщение на бумажный носитель. Сообщение, отправленное в Департамент, при переносе с электронного на бумажный носитель заверяется подписью руководителя Службы внутреннего контроля.

В случаях отсутствия руководителя Службы внутреннего контроля таблица о переданных сообщениях и (или) бумажная копия сообщения подписываются его заместителем либо ответственным сотрудником на основании полномочий, письменно предоставленных ему председателем Правления Банка.

3.3.7. Все переданные в Департамент сообщения и информация в табличной форме о переданных сообщениях должны храниться непосредственно руководителем Службы внутреннего контроля в специально обустроенном помещении или в несгораемом и опечатываемом сейфе.

3.3.8. Также Служба внутреннего контроля должна незамедлительно сообщать в Департамент и по каждой информации подтверждающей подозрительность соответствующей операции или исключающей ее подозрительность.

3.3.9. Если сообщение донесено в неправильной форме или не донесено в полном объеме, а также в случае отсутствия электронной цифровой подписи (печати Банка, подписей ответственных лиц или других обязательных реквизитов), Департамент в дату

получения сообщения направляет запрос о повтороной отправке сообщения, с выполнением требований конфиденциальности и точным указанием недостатков.

После получения из Департамента сообщения такого содержания, Служба внутреннего контроля принимает меры по исправлению указанных в запросе недостатков, и в течение одного дня с момента получения запроса повторно отправляет в Департамент исправленное сообщение.

3.3.10. В случае если Банком были представлены в Департамент ненадлежащие неправильные сведения об операции, Банк направляет в Департамент письменное обращение о том, чтобы считать недействительной представленную информацию.

В сообщении Банка должны быть указаны причины, чтобы считать информацию недействительной, а также сведения позволяющие определить неправильно предоставленную информацию (номер и дата сообщения, способ предоставления, сумма операции, валюта и дата осуществления операции).

3.3.11. Департамент по отправленным сообщениям вправе направлять письменные запросы Банку с затребованием дополнительных сведений и копий заверенных в установленном порядке документов:

в случае возникновения необходимости проверки достоверности полученных сообщений;

в рамках выполнения обязательств по международным договорам Республики Узбекистан, связанным с легализацией доходов, полученных от преступной деятельности, и финансированием терроризма.

Банк после получения таких запросов в течение 3 рабочих дней по запросу Департамента представляет нарочно или через специальную почту заверенные копии запрошенных сведений.

В свою очередь Департамент может определить иные сроки предоставления сведений, исходя из их объема и характеристики.

3.4.Меры принимаемые по обеспечению полноты сведений по международным денежным переводам, а также в случае выявления денежных переводов в иностранной валюте, по которым отсутствуют требуемые данные

3.4.1. Соответствующие подразделения Банка должны принять необходимые меры для полноты и достоверности сведений, требуемых о получателе и (или) отправителе всех международных переводов (платежей).

Международными переводами (платежами) считаются операции связанные с клиентом (или Банком) контрагентом (отправителем или получателем), являющимся физическим или юридическим лицом, или денежными средствами его банка расположенными в зарубежном государстве.

3.4.2. При приеме платежного документа по международному платежу у клиента Банка являющегося юридическим лицом, сотрудник соответствующего подразделения должен обратить внимание на наименование, адрес отправителя денег, цель платежа, а также наименование, страну, адрес, банк (наименование, СВИФТ код, страну) получателя.

3.4.3. При поступлении денежных средств по международным платежам клиенту Банка являющемуся юридическим лицом, соответствующий сотрудник Отдела ведения учета валютных операций осуществляющий валютный контроль юридических лиц, тщательно проверяет документ (СВИФТ извещение), послуживший основанием для оприходования денежных средств, а также обращает внимание наличие и правильное отражение в нем наименования получателя, наименование, страну, адрес банк (наименование, СВИФТ код, страну) отправителя и цель платежа.

3.4.4. В случае полного и правильного отражения требуемых сведений, денежные средства приходуются на счет клиента.

3.4.5. При неполном и неправильном отражении требуемых сведений, Отдел ведения учета валютных операций:

– если не указано наименование получателя или отправителя, принимает меры по направлению запроса банку-нерезиденту по оприходованию средств на транзитный счет и выявлению неполных и неправильно указанных сведений, а также в тот же день в установленном порядке сообщает Службе внутреннего контроля;
– если полностью указано наименование получателя и отправителя, но не указано одно из других требуемых сведений (наименование, адрес, страна отправителя, предмет платежа), принимает меры по направлению запроса банку-нерезиденту по оприходованию средств на транзитный счет и выявлению неполных и неправильно указанных сведений.

3.4.6. С целью организации и контроля международных денежных переводов физических лиц, Управление денежного обращения и розничных операций должно вести учет оказывающих такие услуги подразделений (отделов, мини банков, центров розничных операций) и сотрудников этих подразделений.

До осуществления операций по денежным переводам сотрудники подразделений, оказывающие такие услуги, обязаны надлежащим образом проверить клиентов - физических лиц.

3.4.7. Ответственные сотрудники подразделений, осуществляющих международные денежные переводы, должны обеспечить сопровождение перевода точными сведениями о клиенте-отправителе (фамилия, имя, отчество (если имеется); серия и номер документа, удостоверяющего личность (паспорта или заменяющего его документа); если в процессе операции использовался счет, то его номер или уникальный код операции; адрес отправителя или государственный идентификационный номер либо идентификационный номер клиента или для физических лиц дата и место рождения), и о получателе (фамилия, имя, отчество (если имеется); номер счета, если в процессе операции использовался счет клиента или уникальный номер операции).

3.4.8. Ответственные сотрудники подразделений, осуществляющие международные денежные переводы по международным денежным переводам поступившим клиентам – физическим лицам, в процессе проверки полноты сведений по таким переводам, должны:
– если не указано хотя бы одно из основных сведений, то есть фамилия, имя, отчество (если имеется) или страна отправителя, денежный перевод не выплачивается клиенту, а также в тот же день сообщается о данной операции своему непосредственному руководителю и Службе внутреннего контроля. По платежам, поступившим из отправителя в банках-нерезидентов, об этом делается обращение в Управление денежного обращения и розничных операций. В свою очередь Управление денежного обращения и розничных операций принимает меры по выявлению неуказанных сведений (направляет соответствующие запросы в систему международных денежных переводов или банку-нерезиденту);
– если указано фамилия, имя, отчество (если имеется) и страна отправителя, но не указано одно из других сведений, об этом делается обращение в Управление денежного обращения и розничных операций. В свою очередь Управление денежного обращения и розничных операций принимает меры по выявлению неуказанных сведений (направляет соответствующие запросы в систему международных денежных переводов или банку-нерезиденту).

3.4.9. С целью осуществления эффективного контроля за операциями клиентов и оперативного получения сведений по ним, Управление внешнеэкономической деятельности и Управление денежного обращения и розничных операций должны вести учет по всем международным денежным переводом.

Сведения по всем международным денежным переводам (платежам) юридических и физических лиц должны вестись в виде электронной таблицы и давать возможность при возникновении необходимости получать нужные сведения, а также группировать и отфильтровывать по показателям (стране, сумме, виду платежа и т.д.).

3.4.10. Управление внутреннего контроля, Управление внешнеэкономической деятельности и Управление денежного обращения и розничных операций формируют базу данных по всем международным денежным переводам (платежам) юридических и физических лиц и пользуются ей для анализа, контроля и отчета операций клиента.

3.5.Предоставление сотрудниками внутреннего контроля информации о фактах нарушения закона руководителю Службы внутреннего контроля

3.5.1. Руководитель Службы внутреннего контроля в рамках своих полномочий должен принять необходимые меры для правильной организации и оказания деятельности в Банке по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

Руководитель Службы внутреннего контроля для контролирования организации в филиалах системы внутреннего контроля должен быть в постоянном контакте с закрепленными за ними сотрудниками внутреннего контроля.

3.5.2. Закрепленные за филиалами Банка сотрудники внутреннего контроля, оценивая степень осуществления деятельности системы внутреннего контроля в филиалах, должны принимать соответствующие меры по ее совершенствованию или устранению допускаемых недостатков, в частности по информированию руководителя Службы внутреннего контроля, являющегося непосредственным руководителем.

Сотрудники внутреннего контроля в ходе выполнения своих функций обязаны обратить особое внимание на:

- правильное налаживание надлежащей проверки клиентов сотрудниками соответствующих подразделений, в частности своевременное и полное внесение в электронные анкеты клиентов сведений по их идентификации;
- принятие соответствующих мер сотрудниками соответствующих подразделений в процессе надлежащей проверки клиентов по выявлению публичных должностных лиц;
- своевременное выявление сомнительных операций сотрудниками соответствующих подразделений и сообщение сотрудникам внутреннего контроля;
- своевременное предоставление в Головной банк сведений о подозрительных операциях;
- сообщение руководству о состоянии по внутреннему контролю в банке, в том числе внесение предложений по предоставлению отчетов о сомнительных и подозрительных операциях и совершенствованию системы внутреннего контроля;
- правильное ведение документов в Банке по внутреннему контролю касающемуся противодействию легализации доходов, полученных от преступной деятельности, и финансирования терроризма.

3.5.3. В случае допущения недостатков при выполнении данных задач (идентификация клиентов, заполнение электронных анкет, обновление идентификационных данных, выявление сомнительных и подозрительных операция и сообщение о них, ведение электронных таблиц по международным платежам) сотрудниками филиала, задействованными для выполнения функций по системе внутреннего контроля, сотрудник Службы внутреннего контроля обращается об этом руководителю филиала и руководителю Службы внутреннего контроля с просьбой принятия соответствующих мер к виновным сотрудникам.

При невыполнении сотрудниками филиала требований, установленных настоящими внутренними правилами, допущении грубых ошибок и повторении недостатков, руководитель Службы внутреннего контроля письменно обращается к Председателю Правления с просьбой принять меры к соответствующим сотрудникам.

3.5.4. Сотрудников внутреннего контроля необходимо обеспечить необходимой для выполнения своих функций техническими и программными средствами. Сотрудников внутреннего контроля каждого филиала следует обеспечить отдельной передающей и

принимающей адресной программой Lotus Notes для формирования, отправки Департаменту и получения извещений в виде электронного файла с криптографической защитой.

3.5.5. Сотрудники внутреннего контроля филиалов отправляют сведения о сомнительных и подозрительных операциях Руководителю Службы внутреннего контроля Головного офиса, в форме файла таблицы сформированной программой Excel с установлением пароля. Извещения об операциях, соответствующих критериям подозрительности, также отправляют в виде электронного файла с криптографической защитой.

В случае необходимости, работниками внутреннего контроля Головного офиса могут быть запрошены дополнительные сведения касательно клиенту или проводимых им операций. В подобных случаях работники филиала принимают меры по обеспечению конфиденциальности доставки сведений.

IV.ПОРЯДОК ВЫЯВЛЕНИЯ, ОЦЕНКИ, УПРАВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ УРОВНЯ РИСКА

4.1.Выявление уровня риска клиентов, ведение учета и мониторинг клиентов относящихся к высшему уровню риска

4.1.1. Служба внутреннего контроля должна принимать соответствующие меры по выявлению, оценке, мониторингу, управлению и снижению уровня риска.

Служба внутреннего контроля должна определять общий уровень риска, требуемый уровень его снижения и реализовать соответствующую программу мер в зависимости от типов и уровня рисков.

Служба внутреннего контроля обязана систематически, не менее одного раза в год проводить изучение, анализ и выявление возможных рисков легализации доходов, полученных от преступной деятельности, финансирования терроризма и финансирования распространения оружия массового уничтожения, документально фиксировать результаты изучения.

Служба внутреннего контроля должна определять общий уровень риска, требуемый уровень его снижения и реализовать соответствующую программу мер в зависимости от типов и уровня рисков.

Применяемые меры должны позволять принимать решение о проведении расширенных или упрощенных мер контроля выявленных рисков и эффективном распределении ресурсов.

Уровень риска выявляется и оценивается ответственным сотрудником на основании представленной клиентом информации с учетом видов деятельности и операций, совершаемых клиентом, критериев, установленных настоящими Правилами, результатов надлежащей проверки клиента, факторов риска (по типам и деятельности клиентов, банковским средствам и услугам, каналам поставок, географическим регионам и другие), в том числе на основании изучения и анализа представленных клиентом информаций.

Результаты оценки риска должны быть представлены Центральный банк Республики Узбекистан.

4.1.2. Сотрудник службы внутреннего контроля согласно сведениям, полученным в результате надлежащей проверки сотрудниками подразделений (отдел по корпоративному обслуживанию клиентов, отдел розничных операция и пластиковых карт и др.), непосредственно обслуживающих клиентов, в соответствии с критериями, определенными в настоящих Правилах, определяют клиентам уровень риска на основании выданных сведений о соответствии к категории высокому уровню риска.

4.1.3. С целью своевременного и правильного отнесения клиентов к категории высокого уровня риска, сотрудники Службы внутреннего контроля не позднее рабочего

дня, следующего за днем надлежащей проверки клиента (открытия счета, осуществления разовой операции), основываясь на сведения отраженные в их электронных анкетах, определяет в электронной анкете отнесение или не отнесение их к высокому уровню риска.

Сотрудники Службы внутреннего контроля, проверив документы (юридические папки), отражающие идентификационные сведения юридических лиц и индивидуальных предпринимателей, проверяют полное и правильное введение данных сведений в электронные анкеты.

При необходимости сотрудники Службы внутреннего контроля могут также затребовать и первичные документы физических лиц (заявление, договор, копию документа, подтверждающего личность, и т.п.).

4.1.4. В случае если электронная анкета клиента была не сформирована, сотрудник Службы внутреннего контроля сообщает это начальнику подразделения, ответственному за заполнение электронной анкеты, и требует своевременного заполнения электронной анкеты.

После сформирования электронной анкеты клиента, если клиент согласно критериям, установленным настоящими Правилами, относится к уровню высокого риска, ставит соответствующую отметку в его электронной анкете.

4.1.5. После того, как сотрудник Службы внутреннего контроля поставил отметку в электронной анкете клиента о том, что он отнесен к категории высокого уровня риска, он отпечатывает его анкету в бумажных носителях и для подтверждения сведений, включенных в электронную анкету, предоставляет ее главному бухгалтеру, или в случае его отсутствия, его заместителю либо ответственному сотруднику.

Анкеты, представленные в бумажных носителях, должны быть незамедлительно рассмотрены, и при отсутствии ошибок, подписаны и возвращены обратно.

4.1.6. Сотрудники Службы внутреннего контроля обязаны вести дневной электронные перечни клиентов, у которых не сформированы электронные анкеты и отнесенных к категории высокого уровня риска. В электронном перечне клиентов, отнесенных к категории высокого уровня риска, помимо сведений о клиентах, должен быть отражен критерий, по которому он отнесен к категории высокого уровня риска, дата начала ведения деятельности (по юридическим лицам и индивидуальным предпринимателям), какими видами дистанционных услуг пользуется или не пользуется, дата отнесения к категории высокого уровня риска. Автоматизированная банковская система должна предоставлять возможность получения сведений о клиентах, отнесенных к категории высокого уровня риска.

При повторении случаев несвоевременного заполнения электронных анкет, сотрудник Службы внутреннего контроля обращается об этом к руководителю филиала и руководителю Службы внутреннего контроля, с указанием факторов препятствующих эффективной деятельности системы внутреннего контроля, а также с просьбой принять надлежащие меры к виновным в этом сотрудникам.

4.1.7. В случае если клиент или осуществляемая клиентом операция, отнесены к категории высокого уровня риска, Служба внутреннего контроля обязана вести постоянный мониторинг за операциями, осуществляемыми этим клиентом.

4.1.8. В зависимости от изменения категории операций, осуществляемых клиентом, Служба внутреннего контроля в случае необходимости должно пересмотреть уровень риска по работе с ним.

При исключении сотрудником Службы внутреннего контроля клиента из категории высокого уровня риска, он вносит соответствующее изменение в его электронной анкете и электронном перечне клиентов, отнесенных к категории высокого уровня риска, и убирает его анкету в бумажных носителях из папки анкет клиентов, отнесенных к категории высокого уровня риска.

4.2. Критерии клиентов и операций, отнесенных к категории высокого уровня риска

4.2.1. К категории высокого уровня риска Служба внутреннего контроля обязана отнести клиентов, отвечающих изначально следующим критериям, в отношении которых соответствующие подразделения должны проявлять повышенное внимание:

а) лица, включенные в Перечень либо организации, находящиеся в собственности или под контролем лица, включенного в Перечень, либо лица, прямо или косвенно являющиеся собственниками или контролирующие организацию, включенную в Перечень;

б) лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;

в) представительства иностранных компаний и нерезиденты — физические лица Республики Узбекистан;

г) лица, постоянно проживающие, находящиеся или зарегистрированные в оффшорной зоне;

д) резиденты и нерезиденты, имеющие счета в оффшорных зонах;

е) организации и индивидуальные предприниматели, фактическое местонахождение которых не соответствует сведениям, указанным в учредительных или регистрационных документах;

з) организации, бенефициарным собственником которых является лицо, указанное в подпунктах «а» и «б» настоящего пункта;

и) клиенты, осуществляющие подозрительные или сомнительные операции на систематической основе (например, в течение 3 месяцев подряд);

к) клиенты, использующие программные комплексы, исключающие возможность осуществления надлежащей проверки клиента;

л) публичные должностные лица, члены их семей и лица, близкие к публичным должностным лицам;

м) лица, включенные в действующие перечни ООН (на основании Резолюций Совта Безопасности) и Управления по контролю за зарубежными активами Министерства финансов США (OFAC SDN List) и известные Банку.

4.2.2. К категории высокого уровня риска Банк обязан отнести операции, отвечающие следующим критериям и в отношении которых должен проявлять повышенное внимание:

а) операции, участниками которых являются лица, указанные в подпунктах “а”, “б”, “з”, “л” и “м” пункта 3.2.1 настоящих Правил;

б) операции, осуществляемые через счета, открытые в оффшорных зонах;

в) операции с драгоценными металлами, драгоценными камнями, а также ювелирными изделиями, содержащими драгоценные металлы и драгоценные камни, за исключением таких операций, проводимых самими коммерческими банками;

г) операции, связанные с переводами денежных средств, в которых сведения об отправителе (фамилия, имя, отчество физических лиц, полное наименование юридических лиц, местонахождение (почтовый адрес) и номер счета отправителя) представлены не в полном объеме;

д) операции с банками государств, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, и операции со сторонами зарегистрированными в этих государствах;

е) операции, участниками которых являются лица, указанные в подпунктах "л", "м" пункта 3.2 настоящих Правил.

4.3. Меры направленные на предотвращение использования технологических достижений с целью легализации преступных доходов и (или) финансирования терроризма

4.3.1. Банк должен принять меры направленные на предотвращение использования технологических достижений с целью легализации преступных доходов и (или) финансирования терроризма. В этих целях соответствующие подразделения Банка должны определять и оценивать уровни риска, которые могут возникнуть в связи;

с разработкой новых видов услуг и новой деловой практики;

с использованием новых или развивающихся технологий как для новых, так и для уже существующих видов услуг.

4.3.2. Такая оценка риска должна проводиться до запуска новых видов услуг, деловой практики или использования новых или развивающихся технологий. При этом определение и оценка данного риска должны осуществляться подразделением Банка, непосредственно внедряющим новые виды услуг (новую технологию), совместно со Службой внутреннего контроля.

Данное подразделение Банка и Служба внутреннего контроля должны принимать соответствующие меры для мониторинга и снижения этих рисков.

4.3.3. Подразделение, выступающее с инициативой внедрения в практику новых или развития имеющихся видов услуг и новых рабочих операций, с использованием технологических достижений, предоставляет предложение об этом руководителю филиала, где он осуществляет деятельность. Руководитель филиала рассматривает данное предложение и, при целесообразности его дальнейшего рассмотрения, предоставляет соответствующему управлению (управлениям), контролирующему и координирующему данный вид услуг или рабочую операцию.

Соответствующее управление (управления) или сам предлагающий, помимо анализа удобств и эффективностей возникающей благодаря внедрению новых или имеющихся видов услуг и новых рабочих операций, с использованием технологических достижений, должны выявить и оценить возможный уровень риска.

Соответствующее управление (управления), оценив уровень риска, предоставляют Службе внутреннего контроля предложение по новому виду услуг или рабочей практике, в том числе с подробным освещением технических сторон, для рассмотрения и оценки уровня риска, а также дачи предложения по снижению данного риска.

4.3.4. Служба внутреннего контроля должна подробно изучить все особенности предложения связанного с внедрением нового вида услуг или рабочей операции. При возникновении необходимости, Служба внутреннего контроля вправе запросить помощи у других подразделений Банка (Управление информационных технологий, Юридическое управление и др.).

Служба внутреннего контроля, изучив и оценив риски, предоставляет Правлению Банка письменное заключение с указанием возможных уровней рисков, а также соответствующих мер для мониторинга и снижения этих рисков.

4.3.5. Внедрение новых видов услуг и новых рабочих операций, с применением технологических достижений, осуществляется на основании решения Правления Банка.

4.3.6. В целях снижения риска соответствующие подразделения Банка, предоставляющие дистанционные услуги:

должны в договорах, заключаемых с клиентами об оказании дистанционных услуг, предусмотреть меры (приостановление предоставления данной услуги клиенту до момента письменного объяснения клиента законности проведенных операций; отказ от предоставления данной услуги), принимаемые в случае выявления подозрительных операций, осуществленных клиентом с использованием таких услуг;

вправе осуществлять изучение клиента по месту нахождения (почтового адреса) или адреса, указанного в договоре об оказании дистанционных услуг, в том числе для изучения процесса осуществления операции непосредственно лицом, которое указано в договоре об оказании дистанционных услуг, при наличии сомнений о проведении подозрительных операций с использованием дистанционных услуг;

должны приостановить предоставление дистанционных услуг, с использованием которых осуществлялись подозрительные операции, на срок, указанный в договоре об оказании данной услуги;

должны расторгнуть в установленном порядке договор об оказании дистанционных услуг в случае наличия обоснованных подозрений использования таких услуг в целях легализации доходов, полученных от преступной деятельности, и финансирования терроризма.

4.3.7. При изучении клиента, пользующегося дистанционными услугами, по месту его нахождения (почтовому адресу) или адресу, указанному в договоре об оказании дистанционных услуг, соответствующие подразделения Банка должны уделять особое внимание соблюдению клиентом требований Положения о безналичных расчетах в Республике Узбекистан (рег. № 2465 от 3 июня 2013 года) (Собрание законодательства Республики Узбекистан, 2013 г., № 23, ст. 309), в том числе оформлению расчетных документов, их заверению подписью уполномоченных лиц (руководителя, главного бухгалтера), осуществлению переводов по этим документам только после подтверждения электронно-цифровой подписью лицом, непосредственно имеющим право на электронную подпись, хранению данных документов.

4.3.8. С целью оказания качественных и современных услуг подразделениями Банка, повышения продуктивности труда сотрудников, а также улучшения деятельности системы внутреннего контроля, соответствующими подразделениями должны быть приняты меры по изучению и внедрению современных технологий, облегчению рабочих процессов, совершенствованию имеющегося программного обеспечения, внедрению обоснованных и полезных управленческих видов отчетов.

4.3.9. Служба внутреннего контроля при выполнении своих обязанностей может изучать программные средства используемые другими подразделениями и составляемые ими отчеты, а также вносить предложения руководству Банка по приспособлению их к современным требованиям. Также, в отдельных случаях, при возникновении необходимости, вправе запрашивать с подразделений составить отчеты связанные со своей деятельностью.

4.3.10. База данных, полученная в результате надлежащей проверки клиентов, должна давать возможность оперативного и удобного получения из этих данных полезных отчетов, в частности она должна отвечать следующим требованиям:

- отпечатка в бумажных носителях анкет клиентов;
- поиск и группирование по нескольким показателям (наименование, страна, вид деятельности, адрес и др.) среди всех категорий клиентов;
- автоматическое контролирование на максимальном уровне присвоения определенного уровня риска клиентам на основе имеющихся критериев;
- получение сведений по клиентам и их реальным владельцам в зарегистрированным и проживающим в оффшорных зонах и государствах, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, и др..

4.3.11. Управление информационных технологий принимает соответствующие меры по систематическому совершенствованию используемых в Банке информационных технологий, в частности автоматизированной банковской системы и других программных средств. Служба внутреннего контроля может обращаться в это подразделение по таким вопросам.

V. ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ КЛИЕНТА

5.1. Общие правила цифровой идентификации клиентов

5.1.1. До внедрения цифровой системы идентификации клиентов будут приняты меры по изучению, анализу, выявлению, оценке, мониторингу, управлению,

документированию и снижению потенциального риска отмывания денег, финансирования терроризма и распространения оружия массового уничтожения.
Служба внутреннего контроля проводит анализ и оценку рисков, представляет Правлению Банка письменный отчет с указанием возможных уровней рисков и соответствующих мер по их мониторингу и снижению.

5.1.2. При цифровой идентификации клиентов соответствующие подразделения банка должны принять следующие меры по информационной безопасности:
- необходимые правовые, организационные и технические меры для защиты идентификационных данных клиента;
- обеспечение достоверности и точности идентификационной информации;
- принимать меры против подделки, несанкционированного изменения и разглашения идентификационной информации;
- контроль за хранением и использованием идентификационных данных;
- принимать меры по снижению и контролю операционных рисков, связанных с информационной безопасностью при оказании платежных услуг, в том числе с безопасностью при цифровой идентификации клиентов;
- применение процедур многофакторной аутентификации клиента при использовании банковских услуг (общение по мобильному телефону или отправка SMS или электронной почты, а также дополнительная проверка и подтверждение личности клиента через социальные сети);
- применять необходимые требования в соответствии с другим законодательством в данной области.

5.2. Цифровая идентификация клиентов

5.2.1. Цифровая идентификация распространяется на граждан Республики Узбекистан, иностранных граждан и лиц без гражданства, постоянно или временно проживающих на территории Республики Узбекистан.

5.2.2. Для цифровой идентификации клиентов используются следующие методы:
проверка и идентификация клиента ответственным сотрудником на основании информации, предоставленной клиентом;
проверка в режиме реального времени и идентификация клиента без человеческого фактора информационными системами.

5.2.3. При проверке и идентификации клиента на основе информации, предоставленной клиентом:
- получает от клиента фотографии частей документа, удостоверяющего личность (биометрический паспорт или идентификационная ID-карта или водительское удостоверение нового образца) с соответствующей информацией в соответствии с требованиями правил внутреннего контроля;
- принимает фото и (или) видео клиента в соответствии с установленными требованиями;
- сопоставляет с данными физических и юридических лиц путем направления запроса в центральные базы данных системы «Электронное правительство» (далее - центральная база данных);
- сопоставляет фотографию в документе, удостоверяющем личность, с фото и (или) видео, сделанными в соответствии с настоящими Правилами, а также с фотографией (при наличии), размещенной в центральной базе данных;
- Проверяет номер мобильного телефона, используемый для связи с клиентом, методом, позволяющим определить, используется ли он клиентом (подключение мобильного телефона, отправка SMS);
- в соответствии с правилами внутреннего контроля проверяет, не относится ли клиент к категории высокого риска.
- Ответственный сотрудник устанавливает сеанс онлайн-видеоконференции с клиентом и проверяет принадлежность полученных документов ему.

5.2.4. В режиме реального времени проверка и идентификация клиента без человеческого фактора информационными системами:

а) серия и номер документа, удостоверяющего личность (биометрический паспорт или удостоверение личности или новое водительское удостоверение) или личный код и дата рождения физического лица или вся эта информация и фотография в соответствии с Положением о цифровая идентификация клиентов или захват видео в режиме реального времени;

б) отправляет запрос в центральную базу данных и получает следующую персональную информацию клиента:

цифровая фотография (при наличии);

персональный идентификационный номер физического лица (ИНН);

дата выдачи биометрического паспорта или удостоверения личности, срок его действия и место выдачи;

фамилия, имя, отчество на государственном языке (на латинице);

сведения о поле, стране рождения, месте рождения, национальности, гражданстве и месте постоянного или временного проживания;

в) фото в реальном времени, снятое с заказчика или фото в видео с фото из центральной базы (если есть)

сравнивает автоматически (без человеческого фактора);

г) проверяет номер мобильного телефона, используемый для связи с клиентом, с помощью метода, позволяющего определить, используется ли он клиентом (подключение мобильного телефона, отправка SMS);

д) сравнивает полученные данные со Списком в автоматическом режиме (без учета человеческого фактора) в соответствии с правилами внутреннего контроля.

5.2.5. Соответствующие подразделения Банка обеспечивают соответствие информационных систем, используемых при цифровой идентификации или цифровой аутентификации клиентов, требованиям к полученной через них персональной информации клиента (фото или видео).

5.3. Использование цифровой идентификации

5.3.1. Цифровая идентификация может использоваться для предоставления следующих услуг при соблюдении определенных требований:

открытие и управление электронными кошельками;

открытие и управление банковским счетом, а также банковской картой;

трансграничные денежные переводы с использованием банковских карт или систем электронных денег;

получить онлайн микрозайм.

5.3.2. Строгие ограничения накладываются на следующие операции с клиентами, идентифицированными в цифровой форме, с оценкой уровня риска в соответствии с правилами внутреннего контроля:

- максимальная сумма одной операции, совершаемой владельцем электронных денег;
- максимальное количество электронных денег, хранимых на одном электронном устройстве владельца электронных денег;
- сумма суммы операций, совершенных владельцем электронных денег в течение календарного месяца;
- сумма суммы операций, совершенных владельцем банковского счета (карты) в течение календарного месяца;
- количество транзакций, совершенных владельцем электронных денег и (или) владельцем банковского счета (карты) в течение календарного месяца;
- сумма онлайн микрокредита.

Данные ограничения разрабатываются ответственными подразделениями банка по согласованию со Службой внутреннего контроля и утверждаются Правлением Банка.

Иные ограничения могут быть наложены на цифровую идентификацию клиентов и цифровую аутентификацию ранее идентифицированных клиентов Службой внутреннего контроля, оценивая уровень риска операций каждого клиента.

5.3.3. В случае обнаружения попыток клиентов обойти установленные ограничения, должны быть приняты меры к прекращению любых практических деловых отношений с таким клиентом или к отказу от его операций.

5.3.4. Клиенты не идентифицируются в цифровой форме в следующих случаях:

- в случае, если операция, совершаемая клиентом и (или) клиентом, отнесена к категории высокого риска в соответствии с правилами внутреннего контроля;
- при возникновении сомнений в достоверности информации, предоставленной клиентом;
- при наличии сомнения в том, что фотография в документе, удостоверяющем личность, соответствует фотографии и (или) видео, сделанным в соответствии с Положением «О порядке цифровой идентификации клиентов» и фотографии (при наличии), размещенной в центральной базе данных;
- когда данные, полученные от клиента, не соответствуют данным, размещенным в центральной базе данных, или невозможность проверки соответствия;
- несоответствие фото и (или) видеозаписи требованиям Положения «О порядке цифровой идентификации клиентов»;
- при наличии сомнений в легализации доходов от преступной деятельности, финансировании терроризма и финансировании распространения оружия массового поражения.

5.3.5. При цифровой идентификации в случае частичного или полного соответствия всех идентификационных данных клиента данным Зарегистрированного лица принимаются меры в соответствии с разделом VI Правил внутреннего контроля.

5.3.6. Заполнение и ведение анкеты клиента по результатам цифровой идентификации клиента осуществляется в соответствии с требованиями, установленными правилами внутреннего контроля.

5.3.7. Помимо информации, требуемой правилами внутреннего контроля для клиентов, идентифицированных в цифровой форме, фото и (или) видео, снятые с клиентов, документы, указывающие точную дату и время проверки и идентификации клиента, а также результаты проверки данных с использованием центральная база данных анкет клиентов вместе в течение пяти лет в соответствии с правилами внутреннего контроля.

VI. ПОРЯДОК КОНТРОЛЯ НАД ОПЕРАЦИЯМИ ЛИЦ, ВКЛЮЧЕННЫХ В ПЕРЕЧЕНЬ

6.1. Меры, принимаемые при выявлении операций с участием лиц, включенных в Перечень

6.1.1 При осуществлении операций ответственные сотрудники соответствующих подразделений Банка обязаны сверять идентификационные сведения участников операций с Перечнем.

В случае полного совпадения всех идентификационных данных клиента или одного из участников операции с данными лица, включенными в Перечень, Банк безотлагательно и без уведомления приостанавливает эту операцию (за исключением операций по включению поступивших денежных средств на счет юридического или физического лица) и (или) замораживает денежные средства или другое имущество.

Под полным совпадением понимается точное и однозначное соответствие имеющихся идентификационных данных клиента или одного из участников операции всем соответствующим сведениям, содержащимся в Перечне.

Операция с денежными средствами или иным имуществом также подлежит приостановлению, а денежные средства или иное имущество замораживанию, в случаях, если:

один из ее участников действует от имени или по поручению лица, включенного в Перечень;

денежные средства или иное имущество, используемые для проведения операции, полностью или частично принадлежат или контролируются лицом, включенным в Перечень;

денежные средства или иное имущество получены или приобретены путем использования денежных средств или иного имущества, прямо или косвенно принадлежащих или контролируемых лицами, включенными в Перечень;

юридическое лицо – участник операции, находится в собственности или под контролем физического или юридического лица, включенного в Перечень.

6.1.2. Служба внутреннего контроля при приостановлении операции и (или) замораживании денежных средств или иного имущества лица, включенного в Перечень, обязана не позднее одного рабочего дня направить сообщение о подозрительной операции в Департамент, с указанием суммы замороженного имущества.

6.1.3. Если во время установления отношений или при проведении операции, сотрудниками Банка будет установлено полное совпадение всех идентификационных данных клиента или одного из участников операции с лицом, включенным в Перечень, они должны безотлагательно и без уведомления клиента сообщить об этом Службе внутреннего контроля. В свою очередь Служба внутреннего контроля должна предпринять следующие меры по:

подробной идентификации личности клиента, бенефициарного собственника клиента либо одного из участников операции, по мере возможности;

выявлению денежных средств или иного имущества по операции, подлежащих замораживанию в соответствии с требованиями законодательства и настоящих Правил;

подготовке и внесению на подпись руководства банка распоряжения о приостановлении операции, за исключением операций по зачислению денежных средств, поступивших на счет юридического или физического лица, и замораживанию денежных средств или иного имущества по такой операции;

подготовке и отправке в Департамент сообщение о подозрительной операции, связанной с денежными средствами или иным имуществом, в день приостановления операции;

получению дополнительной информации о клиенте (в том числе род деятельности, размер активов, информация, доступная через открытые базы данных и т. п.);

определению источника денежных средств или источника финансового состояния клиента, в том числе путем получения от клиента информации;

занесению информации об операции в специальный журнал.

Ответственные сотрудники Банка вправе проинформировать лицо, включенное в Перечень, о приостановлении его операции и (или) замораживании денежных средств или иного имущества, только после выполнения мер, предусмотренных настоящим пунктом.

6.1.4. В случае приостановления операции денежные средства или иное имущество по заявлению клиента не предоставляются .

Заявление клиента должно регистрироваться в соответствии с указанной в приложении № 10 формой в отдельном журнале по регистрации заявлений клиентов, операции которых приостановлены, а также помещаться в специальную папку до момента возобновления операции.

В отдельном журнале для регистрации заявлений клиентов, операции которых приостановлены, фиксируется информация, позволяющая идентифицировать операцию, которая была приостановлена, а также участников данной операции.

6.1.5. Банк возобновляет проведение приостановленной операции и предоставляет доступ к замороженному имуществу в порядке, установленном Положением о порядке приостановления операций, замораживания денежных средств или иного имущества, предоставления доступа к замороженному имуществу и возобновления операций лиц,

включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения (рег. № 3327 от 19 октября 2021 года).

6.1.6. Служба внутреннего контроля обеспечивает обновление Перечня внутри АБС системы Банка на регулярной основе, при каждом обновлении Перечня, но не реже одного раза в три месяца, осуществлять мониторинг имеющейся базы данных клиентов и их бенифициарных собственников, в целях выявления денежных средств или иного имущества лиц, подлежащих замораживанию каждый раз при обновлении Перечня, а также не реже одного раза в три месяца.

6.2. Возобновление операций связанных с приостановленными денежными средствами или другим имуществом и размораживание имущества лиц, включенных в Перечень. Направление в Департамент обращений, выданных для размораживания приостановленных денежных средств или другого имущества

6.2.1. Организация, осуществляющая операции с денежными средствами или иным имуществом, возобновляет приостановленную операцию и (или) размораживает денежные средства или иное имущество в день получения следующей информации, но не позднее следующего рабочего дня:

об исключении лица из Перечня;

уведомления Департамента о подтверждении "ложного срабатывания".

6.2.2. Лицо, включенное в Перечень, или другой участник операции вправе обратиться к Банку, для получения доступа к замороженному имуществу, в следующих целях:

а) покупки продуктов питания, лекарственных средств и изделий медицинского назначения, оплаты за аренду жилья, ипотечный кредит, коммунальные платежи, медицинские услуги, налоги и сборы, страховые платежи, услуги адвокатов и юридической консультации в пределах средних рыночных цен, текущие платежи и сборы, связанные с обслуживанием банковских счетов или содержанием имущества;

б) оплаты чрезвычайных расходов;

в) предусмотренных в резолюциях Совета Безопасности ООН 1718 (2006), 1737 (2006), 2231 (2015) и резолюциях, принятых в их развитие.

К обращению прилагаются сведения о цели, сумме и обосновании платежа, какую часть из замороженного имущества предполагается использовать, реквизиты и идентификационные данные получателя денежных средств или иного имущества, банке получателе денежных средств.

6.2.3. Служба внутреннего контроля не позднее одного рабочего дня после получения обращения направляет его в Департамент.

Департамент после установленных в законодательстве мер информирует Банк о принятом решении.

В свою очередь Банк в тот же день поступления сообщения из Департамента, но не позднее рабочего дня, следующего за днем поступления, исполняет решение Департамента и информирует об этом клиента.

6.2.4. Операция, связанная с использованием денежных средств или иного имущества, к которым предоставлен доступ, включая попытку ее проведения, сообщается ответственным сотрудником сотруднику Службы внутреннего контроля, и признается Службой внутреннего контроля подозрительной и подлежит сообщению в Департамент в порядке, установленном законодательством.

6.3 Технический порядок работы с программой SWIFT Transaction Screening Utility для эксплуатации транзакций с участием лиц находящихся в Списках.

6.3.1. SWIFT Transaction Screening Utility проверяет совместимость платежей отправителя и получателя с выбранными международными Списками.

6.3.2. Полномочия по своевременному утверждению или отклонению платежей отправителей и получателей в иностранной валюте с использованием программного обеспечения SWIFT Transaction Screening Utility возложены на сотрудников Управления комплаенс-контроля (далее - сотрудников) в соответствии с решением Председателя Правления.

Должность администратора программного обеспечения SWIFT Transaction Screening Utility (супервайзер) закрепляется за начальником Управления комплаенс-контроля, начальником отдела развития и координации системы финансового мониторинга, начальником отдела запросно-санкционных списков (далее - ответственный сотрудник).

6.3.3. Программное обеспечение SWIFT Transaction Screening Utility проверяет действительность заблокированных платежей из-за возможного сходства с лицами в международных списках и принимает независимое решение о том, следует ли переводить этот платеж.

6.3.4. При совпадении сведений об отправителе и получателе платежей с лицами, включенными в список, персоналом принимаются меры, т.е. проверяется точное соответствие аналогичных сведений, изучается дополнительная информация, полученная из открытых источников. Когда проверка установит, что перечисленные лица полностью соответствуют требованиям, ответственный сотрудник примет решение не переводить платеж через программное обеспечение через SWIFT Transaction Screening Utility. Не проведенные платежи возвращаются Департаментом внешнеэкономических связей на счет клиента в соответствии с правилами внутреннего контроля или на счет иностранного банка с причиной «DUE TO INTERNAL POLICY».

VII. ОФОРМЛЕНИЕ, ХРАНЕНИЕ, ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ И ДОКУМЕНТОВ, ПОЛУЧЕННЫХ В РЕЗУЛЬТАТЕ ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

7.1. В Банке и его филиалах должно быть приведено в единую систему оформление и хранение документов внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

7.2. Для хранения документов внутреннего контроля в Банке и его филиалах сотрудниками Службы внутреннего контроля ведутся следующие папки и журналы:

1) анкеты клиентов – являющихся физическими лицами;
2) анкеты клиентов – являющихся индивидуальными предпринимателями;
3) анкеты клиентов – являющихся юридическими лицами;
4) документы, собранные по установлению корреспондентских отношений и банкам-корреспондентам (только в Головном банке);
5) документы по установлению отношений с системами международных денежных переводов и их надлежащей проверке (только в Головном банке);
6) сообщения сотрудников о сомнительных операциях клиентов;
7) по переданным в Департамент сообщениям в отношении подозрительных операций (только в Головном банке);
8) поручения клиентов с приостановленными операциями;
9) сведения, связанные с проверкой или анализом операций клиента;
10) сведения, переданные руководству Банка;
11) переписка с руководством и другими подразделениями Банка;
12) обязательства принятых на работу сотрудников об ознакомлении с правилами внутреннего контроля и соблюдении данных правил;
13) журнал регистрации сообщений сотрудников о сомнительных операциях клиентов;
14) журнал регистрации сообщенных Департаменту подозрительных операций (только в Головном банке);
15) журнал регистрации поручений клиентов с приостановленными операциями;

16) решения руководителя Службы внутреннего контроля о переводе сомнительных операций в подозрительные (только в Головном банке);
17) запросы Департамента по клиентам;
18) переданный Департаментом перечень лиц, связанных с террористической деятельностью;
19) переданный Департаментом перечень государств, не участвующих в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансирования терроризма.

В перечисленных сборниках документы сшиты в хронологическом порядке.

7.3. порядок принятия соответствующих мер по выявлению, оценке, мониторингу, управлению, снижению и документированию рисков;

7.4. документы, связанные с надлежащей проверкой клиентов, составленные полностью или в какой-либо их части на иностранном языке, должны быть истребованы небанковской кредитной организацией, при необходимости, с переводом на государственный или русский язык.

7.5. В случае возникновения сомнений в достоверности представленных копий документов или другой необходимости небанковская кредитная организация вправе потребовать представления подлинников документов для ознакомления.

7.6. Информация о клиенте, полученная в процессе надлежащей проверки клиента, указывается в анкете клиента согласно приложению № 3 к настоящим Правилам.

7.7. Электронные анкеты физических лиц заполняются сотрудниками соответствующих подразделений (сберегательного, валютно-обменного, кассового, кредитного и т.д.), на которых возложены эти задачи.

Ответственные сотрудники соответствующего подразделения, выполняющие надлежащую проверку клиентов в ходе осуществления разовой операции, на верхней левой части обратной стороны копий документов, подтверждающих личность клиентов, записывают дату и сумму операции, и в хронологическом порядке подшиваются в отдельные папки по каждому виду операций (снятие наличности с пластиковых карточек других банков, перевод платежей с пластиковых карточек других банков, перевод платежей через транзитный счет без открытия клиенту лицевого счета и др.). По операциям связанным с пластиковыми карточками ответственными сотрудниками может браться копия чека полученного с терминала без записи вручную даты и суммы операции на обратную сторону копии документа.

Кроме этого, ответственные сотрудники, осуществляющие надлежащую проверку клиентов, по деталям подлежащим идентификации разовых операций клиента должны ежедневно вносить в электронном виде по форме, указанной в приложении № 11, операции по снятию через расположенный в Банке терминал наличности с пластиковых карточек эмиссионных другими банками, по форме, указанной в приложении № 12, платежи за товары и услуги осуществленные через расположенный в Банке терминал с пластиковых карточек эмиссионных другими банками, по форме, указанной в приложении № 13, безналичные платежи за товары и услуги осуществленные физическими лицами без открытия лицевого счета (через транзитные счета).

7.8. Электронные анкеты предпринимателей и юридических лиц заполняются сотрудниками Отдела по оказанию корпоративных услуг юридическим лицам.

7.9. Электронная анкета клиента заполняется ответственным сотрудником, осуществившим идентификацию клиента, или начальником отдела, в котором он работает. В некоторых случаях (например, при отсутствии компьютера у сотрудника, осуществившего идентификацию, или отсутствии возможности у компьютера, за которым он работает, входа в СБД и т.п.), управляющим филиалом заполнение электронной анкеты клиента может быть возложено на другого сотрудника. Однако данная задача должна быть указана в должностной инструкции сотрудника, на которого она возложена, или закреплена приказом.

7.10. При заполнении электронных анкет клиентов – физических и юридических лиц, ответственные сотрудники должны вносить соответствующие сведения о клиенте в программные средства, а также полностью и правильно отражать их в электронной анкете, с соблюдением требований, указанных в приложении № 6.

Сведения в анкете должны заполняться сотрудниками в установленном порядке как можно полностью и разборчиво. Не допускается неправильное или неполное заполнение сотрудником, с преследованием личных интересов с клиентом.

Руководители соответствующих отделов должны обеспечить сотрудников необходимыми первичными документами для заполнения анкет, а также предпринять необходимые меры для их полной сохранности.

7.11. Сотрудники службы внутреннего контроля с целью изучения правильного отражения сведений в анкете клиента, вправе затребовать от соответствующих сотрудников юридические папки, карточки и образцами подписи и оттиска печати, копии документов (паспорт или заменяющий его документ) подтверждающих личность лица, уполномоченного расписываться в денежно-расчетные документы и др. Данные сотрудники обязаны своевременно представлять такие документы при их затребовании.

7.12. Анкеты заполняются в электронном виде на всех клиентов (за исключением клиентов, по которым не требуется проведения мер надлежащей проверки) с помощью специальных программ. На клиентов, осуществляющих сомнительные и (или) подозрительные операции, и на клиентов, отнесенных к категории высокого уровня риска, анкеты заполняются также на бумажном носителе.

Анкета клиента, заполненная в электронном виде, при переносе на бумажный носитель заверяется подписью главного бухгалтера или в случаях отсутствия главного бухгалтера его заместителем либо ответственным сотрудником.

7.13. Анкеты, заполненные в электронном виде, хранятся в электронной базе данных, позволяющей сотрудникам коммерческого банка, осуществляющим идентификацию клиента, а также платежным агентам и платежным субагентам иметь оперативный доступ в постоянном режиме для проверки информации о клиенте.

7.14. Анкета клиента хранится не менее пяти лет со дня прекращения отношений с клиентом.

7.15. По мере изменения указываемой в анкете клиента информации, а также характера проводимых им финансовых операций, Служба внутреннего контроля при необходимости пересматривают уровень риска работы с ним.

7.16. Информация об операциях должна быть оформлена таким образом, чтобы в случае необходимости было возможно восстановить детали операции., Служба внутреннего контроля и Управление информационных технологий совместно с соответствующими подразделениями должны принять все необходимые меры для предоставления в программном обеспечении банка доступа к качественному и оперативному получению отчетов об операциях (международных платежах, аккредитивах, денежных переводах, операциях через пластиковые карточки, сомнительных и подозрительных операциях и др.).

7.17. Соответствующие подразделения банка обязаны хранить информацию об операциях, а также идентификационные данные и материалы по надлежащей проверке клиентов в течение сроков, установленных законодательством, но не менее пяти лет после осуществления операций или прекращения деловых отношений с клиентами.

7.18. Руководитель Службы внутреннего контроля с целью оформления осуществляемых мер должен обеспечить всех сотрудников в филиалах специальными журналами, приведенными в приложении № 8.

Специальный журнал должен быть прошит, пронумерован, с указанием на его обратной стороне количества страниц, даты (год, месяц, день) начала ведения журнала, и заверен подписью руководителя Службы внутреннего контроля.

7.19. В целях ограничения доступа к документам (переписка с Центральным банком и Департаментом, в том числе бумажные и электронные копии переданных в Департамент

сообщений; бумажные и электронные анкеты клиентов; журналы и др.), использованным в деятельности Службы внутреннего контроля (ответственного сотрудника), такие документы и их опись должны храниться непосредственно Службой внутреннего контроля (ответственным сотрудником) в специально обустроенных помещениях или в несгораемом и опечатываемом сейфе в течение сроков, установленных законодательством, но не менее пяти лет.

По истечении сроков хранения документы сдаются в установленном порядке в архив коммерческого банка.

7.20. Электронные версии документов должны архивироваться программным способом, записываться на электронные носители и храниться руководителем Службы внутреннего контроля вместе с описью в несгораемом и опечатываемом сейфе. По итогам каждого месяца Службой внутренего контроля должны архивироваться и записываться на CD или DVD компакт-диски следующие электронные файлы:

а) Clients-list(ГГГГ-ММ) – в порядке роста список клиентов на конец квартала;
б) High-Risk(ГГГГ-ММ) – в порядке роста список клиентов включенных в категорию высокого риска на конец квартала;
в) Terrorists-list(ГГГГ-ММ) – в порядке роста представленный Департаментом список лиц связанных с террористической деятельностью на конец квартала;
г) Messages(ГГГГ-ММ) – в порядке роста с начала года список сообщений по сомнительным и подозрительным операциям на конец квартала;
д) в папках Incoming-messages и Outgoing-messages соответственно хранятся сообщения поступившие с филиалов и сообщения отправленные в Департамент в течение квартала;
е) в папке Reports(ГГГГ-ММ) хранятся в порядке роста помесячно и с начала года за прошедший квартал отчеты представленные в Центральный банк;
ж) в папке Requests(ГГГГ-ММ) поступившие в течение квартала запросы по клиентам храняться отдельно в папках наименованных в формате «ГГГГ-ММ-дд_(способ поступления)_(количество лиц)».

7.21. Сотрудники банка ограничивают доступ к информации, связанной с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма, в том числе к документам, хранящимся в архивах Банка, обеспечивают ее нераспространение и не вправе информировать юридических и физических лиц о предоставлении сообщений об их операциях в Департамент.

Они обеспечивает неразглашение (или не использование в личных целях либо в интересах третьих лиц) информации, полученной в процессе выполнения ими функций по внутреннему контролю.

7.22. Передача информации, в том числе из анкеты, составляющей идентификационные данные клиента, третьим лицам осуществляется в соответствии с законодательством.

7.23. Сведения, полученные в результате надлежащей проверки и идентификации клиента, должны обновляться не реже одного раза в год в случаях, когда Банк оценивает риск осуществления клиентом легализации доходов, полученных от преступной деятельности, или финансирования терроризма, как высокий, в иных случаях не реже одного раза в три года и при наличии изменений в сведениях клиента.

7.24. Сведения, полученные в результате надлежащей проверки клиента, осуществившего разовую операцию, обновляются при следующем осуществлении операции, по которой требуется принятие мер надлежащей проверки клиента.

7.25. Банк должен обеспечить соблюдение платежными агентами и платежными субагентами требований настоящих Правил и внутренних правил

7.26. Банк несет ответственность за нарушение своими платежными агентами и платежными субагентами требований настоящих Правил

7.27. В электронном виде должны регистрироваться и храниться следующие сведения:

а) представленный Департаментом список лиц;
б) выявленные сомнительные операции;
в) сообщенные в Департамент подозрительные операции;
г) клиенты, включенные в категорию высокого риска;
д) международные платежи, в том числе операции по международным денежным переводам;
е) операции по международным пластиковым карточкам.

VIII. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ К ПОДГОТОВКЕ И ОБУЧЕНИЮ КАДРОВ ВНУТРЕННЕГО КОНТРОЛЯ

8.1. Коммерческие банки обязаны проводить регулярную переподготовку сотрудников Службы внутреннего контроля, подразделений банка непосредственно обслуживающих клиентов (ответственные исполнители, кассиры и т. п.), юридических служб, служб внутреннего аудита и безопасности, с целью обеспечения информированности сотрудников о последних новинках, включая информацию по современной технике легализации доходов, полученных от преступной деятельности, и финансирования терроризма, методах и тенденциях, и четкого разъяснения всех аспектов законодательства и обязательств по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

8.2. Служба внутреннего контроля совместно с соответствующими подразделениями Банка ежегодно разрабатывает программу подготовки, переподготовки и обучения сотрудников коммерческого банка по вопросам противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма (далее — программа обучения). Данная программа должна предусматривать следующее:

- порядок проведения обучения, его формы (первичный инструктаж, плановое и внеплановое обучение) и сроки;
- назначение лиц, ответственных за организацию проведения обучения;
- порядок проверки знаний.

Программа обучения утверждается правлением Банка.

8.3. Пред вступлением к исполнению своих служебных обязанностей работников принятых на работу в подразделения, непосредственно осуществляющих банковские операции (отделы розничных операций, пластиковых карт, денежного обращения, корпоративного обслуживания юридических лиц, кредитования, валютных операций, бэк-офис, касса, минибанки и т.п.) сотрудник службы внутреннего контроля обязан провести первичных инструктаж по вопросам противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

Начальник отдела по работе с персоналом или исполняющих его обязанности работник обязан направить принятых на работу в подразделения, непосредственно осуществляющих банковские операции работников для получения первичного инструктажа к сотруднику Службы внутреннего контроля.

8.4. Первичный инструктаж включает в себя следующие вопросы:

- правила надлежащей проверки клиентов;
- сущность присвоения категории риска клиента, критерии клиентов и операций, относящихся к высокому уровню риска;
- критерии и признаки сомнительных и подозрительных операций, действия работника при выявлении подобных операций;
- требования по обеспечению конфиденциальности информации по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма;
- прочее.

Сотрудник прошедший первичный инструктаж, подписывает обязательство по форме приложения № 15, об ознакомлении и соблюдении правил противодействия

легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

8.5. Служба внутреннего контроля совместно с Отделом по работе с персоналом и другими управлениями обязан разработать учебных план семинаров включающий вопросы противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, а также предупреждения правонарушений, совершаемых работниками банка.

Плановое обучение необходимо проводить в каждом филиале не менее одного раза в квартал. Тематика планового обучения должна быть разнообразной и кроме правил внутреннего контроля охватить вопросы о международных требованиях и организациях противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма, недостатков и упущений, допускаемых в подразделениях Банка (отделах кредитования, денежного обращения, корпоративного обслуживания юридических лиц, валютных операций и т.п.), техническим сферам , осуществляемым в целях улучшения качества обслуживание клиентов и усиления внутреннего контроля.

8.6. В случае изменения законодательства по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма или введении новшеств в данную сферу, при разработке или внедрении новой деловой практики с целью повышения эффективности системы Службы внутреннего контроля Банка, или по указанию Председателя Правления могут быть организованы внеплановые учебные занятия.

8.7. С целью повышения эффективности и привлекательности учебных занятий по теме противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма необходимо использовать интерактивные методы обучения, в частности слайды, раздаточные материалы и т.п.

8.8. Банк обязан проводить регулярную переподготовку сотрудников, с целью обеспечения информированности сотрудников о последних новинках, включая информацию по современной технике легализации доходов, полученных от преступной деятельности, и финансирования терроризма, методах и тенденциях, и четкого разъяснения всех аспектов законодательства и обязательств по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

8.9. С целью проверки знаний по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма сотрудников, осуществляющих операции Банк необходимо проводить их аттестацию в соответствии со сроками и порядком, установленной программой, утвержденной Правлением Банка.

8.10. В должностных инструкциях всех работников, осуществляющих банковские операции, необходимо отразить следующие требования:

- факты и порядок надлежащей проверки клиента, знание критериев сомнительных и подозрительных операций, а также клиентов относящихся к категории высокого риска;
- немедленное представление извещения Службе внутреннего контроля и непосредственному руководителю в случае выявления сомнительных и подозрительных операций;
- при обращении к сотруднику, непосредственно обслуживающему клиента, о предоставлении дополнительных сведений по поручению Службы внутреннего контроля, в установленном порядке обратиться к клиенту и довести полученную информацию Службе внутреннего контроля;
- своевременно и правильно осуществлять идентификацию клиента и заполнение электронной анкеты (для работников, на кого возложены эти обязанности).

8.11. Руководитель Службы внутреннего контроля для повышения собственных знаний и квалификации, а также знаний и квалификации сотрудников и ознакомления с последними новинками обязан организовать техническую учебу. Кроме того, оценивая

знания сотрудников, в необходимых случаях принимать меры по направлению сотрудников, нуждающихся в повышении знаний, в учебные курсы.

Руководитель Службы внутреннего контроля обязан владеть современными знаниями и последними новинками и требованиями в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма. В этих целях руководитель Службы внутреннего контроля совместно с Управлением по работе с персоналом принимает меры по поиску и принятию участия в международных курсах и семинарах, и вправе вносить предложение Председателю Правления об участии в них.

IX. ВЗАИМООТНОШЕНИЕ СЛУЖБЫ ВНУТРЕННЕГО КОНТРОЛЯ С ДРУГИМИ ПОДРАЗДЕЛЕНИЯМИ БАНКА

9.1. При осуществлении своей деятельности Служба внутреннего контроля вступает во взаимоотношение с другими подразделениями.

9.2. Служба внутреннего контроля взаимодействует с Управлением бухгалтерского учета и отчетности, Управлением денежного обращения и розничных операций, а также в филиалах с отделами Корпоративного обслуживания юридических лиц, Розничных операций и обслуживания пластиковых карточек, Кассовых операций по следующим вопросам:

- соответствующие сотрудники указанных подразделений осуществляют идентификацию клиентов и их реальных владельцев, полученные сведения с помощью программ вносит в анкету (карточку) клиента;
- по запросу Службы внутреннего контроля представляет документы (юридические папки), полученные в результате надлежащей проверки клиентов;
- соответствующие сотрудники указанных подразделений могут обратиться в службу внутреннего контроля для уточнения сведений, полученных по публичным должностным лицам, выявленным в процессе надлежащей проверки клиентов.

9.3. Служба внутреннего контроля вступает во взаимоотношения с подразделениями по внешне экономической деятельности, кредитования, денежного обращения, обслуживанию пластиковых карт по следующим вопросам:

- работники указанных подразделений по запросу Службы внутреннего контроля для проведения анализа сомнительных операций или проверки операций клиента представляют соответствующие документы (экспортно-импортные контракты, документарные операции, папки по конвертациям, кредитные папки, документы, собранные по перечислениям доходов населения на вкладные счета);
- предоставляют отчеты необходимые Службе внутреннего контроля.

9.4. С Управлением информационных технологий вступает во взаимоотношения по следующим вопросам:

- Управление информационных технологий для выполнения Службой внутреннего контроля своих функций обеспечивает компьютерной технологией, средствами связи, программами и иными техническими средствами, принимает меры по созданию возможности использования всех видов данных имеющихся в автоматизированной системе банка;
- Управление информационных технологий по запросу Службы внутреннего контроля создает и совершенствует программные обеспечения, необходимые для его деятельности (базу данных по клиентам, содействующие выявлению сомнительных и подозрительных операций и т.п.);

9.5. Все подразделения Банка, работающие с клиентами, взаимодействуют со Службой внутреннего контроля по следующим вопросам:

- при выявлении вовремя текущей проверки операций клиента сомнительных операций, обязаны незамедлительно в письменном виде сообщить о таких

операциях своему непосредственному руководителю и сотрудникам Службы внутреннего контроля;

– при выявлении сомнительных операций по поручению Службы внутреннего контроля при необходимости обращаются к клиенту за дополнительными сведениями о проводимой операции;

9.6. Управления Банка, контролирующие и координирующие деятельность всех отделов вовлеченных в систему внутреннего контроля, особенно Управление бухгалтерского учета и отчетности, Управление денежного обращения и розничных операций, Управление внешнеэкономической деятельности и другие управления также должны контролировать и выполнение соответствующими подконтрольными отделами в филиалах требований законодательства по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма. Кроме этого, при обращении Службы внутреннего контроля к управлениям по устранению недостатков допускаемых подконтрольными им соответствующими отделами, путям усиления контроля соответствующими отделами, они должны проявить солидарность и принять соответствующие меры.

9.7. Кроме того Служба внутреннего контроля сотрудничает:

– с Управлением по управлению Банковскими рисками в предотвращении ошибок и нарушений могущих возникнут в результате операционного и кредитного риска, разработке проектов внутренних актов и определении должностных обязанностей сотрудников банка;

– с Управлением Банковской безопасности по вопросу проведения проверок с целью анализа операций клиента;

– с Юридическим управлением по правовым вопросам, с целью изучения типичных случаев нарушений нормативных актов и законодательства Республики;

– с Управлением по работе с персоналом по вопросам обучения сотрудников, повышения их профессионального мастерства, а также по проведению технической учебы и тестов.

9.8. Управление внутреннего аудита сообщает Службе внутреннего контроля недостатки, выявленные в ходе проверок деятельности подразделений Банка, в частности о фактах проведения операций с целью легализации преступных доходов и случаях их сокрытия для принятия по ним соответствующих мер. Также вносит свои предложения по дальнейшему совершенствованию системы внутреннего контроля в Банке.

Служба внутреннего контроля вправе консультироваться с Управлением внутреннего аудита по вопросам, возникающим в процессе деятельности, а также по иным вопросам.

X. ОСУЩЕСТВЛЕНИЕ КОНТРОЛЯ НАД ИСПОЛНЕНИЕМ ПРАВИЛ ВНУТРЕННЕГО КОНТРОЛЯ

10.1. Мониторинг и контроль за соблюдением коммерческими банками требований настоящих Правил осуществляются Службой внутреннего контроля.

10.2. На основании плана, составленного сотрудниками Службы внутреннего контроля в филиалах проводятся проверки по эффективности деятельности системы внутреннего контроля и соблюдения требований настоящих Правил не менее одного раза в год. Во вновь открытых филиалах с целью изначальной правильной организации системы внутреннего контроля проверка проводится не позднее трех месяцев со дня открытия филиала.

В случае направления на проверку руководителя службы внутреннего контроля его обязанности выполняет другой работник Службы внутреннего контроля.

10.3. С целью контроля выполнения Банком и его филиалами требований правил внутреннего контроля по противодействию легализации доходов, полученных от

преступной деятельности, и финансированию терроризма, сотрудники Службы внутреннего контроля обязаны проводить по завершению каждого месяца до 10 числе следующего месяца промежуточный мониторинг. При осуществлении промежуточного мониторинга они обязаны уделить внимание следующим вопросам:

- правильность надлежащей проверки клиентов, в том числе по разовым операциям;
- принятие соответствующих мер по выявлению публичных должностных лиц в процессе надлежащей проверки клиентов;
- своевременное и правильное заполнение электронных анкет клиентов;
- своевременное внесение соответствующих изменений в электронные анкеты клиентов, в случаях изменения идентификационных данных клиента;
- своевременное полное извещение об операциях, отвечающих критериям сомнительных и подозрительных операций по экспортно-импортным контрактам и международным платежам;
- полное извещение о сомнительных и подозрительных операциях по денежным переводам физических лиц;
- полное извещение о сомнительных и подозрительных операциях по пластиковым картам;
- полное и своевременное извещение об осуществленных в национальной валюте операциях, имеющих критерии и признаки сомнительности или подозрительности, предусмотренные в пунктах 4.1.1-4.1.2 к настоящим Правилам;
- иные вопросы.

При затребовании сотрудниками службы внутреннего контроля сведений и документов, запрошенных в рамках вопросов, включающих промежуточный мониторинг, в том числе юридических папок, идентификационных сведений, электронных форм некоторых операций и других, они должны быть своевременно предоставлены соответствующими управлениями и отделами.

10.4. В случае выявления сомнительных и подозрительных операций во время проведения промежуточного мониторинга сотрудниками Службы внутреннего контроля, необходимо обратить внимание на предоставление в установленном порядке сообщения о них соответствующими работниками.

Сомнительные и подозрительные операции, по которым не были представлены сообщения, изучаются и принимается по ним соответствующее решение. После этого устанавливается причина своевременного непредставления информации об этих операциях работникам службы внутреннего контроля.

10.5. Соответствующие работники Банка несут ответственность за непредставление информации о сомнительных операциях и за их сокрытие.

10.6. По результатам промежуточного мониторинга составляется справка, и ее копии не позднее 12 числа месяца в установленном порядке предоставляются руководителю службы внутреннего контроля и управляющему филиала.

Управляющим филиалом изучаются выявленные недостатки, и сообщаются начальникам соответствующих отделов, а также принимаются меры по их устранению и не допущению в будущем.

Руководитель службы внутреннего контроля изучает результаты месячного мониторинга, проведенного во всех филиалах сотрудниками службы внутреннего контроля, составляет сводную справку и не позднее 15 числа месяца представляет Председателю Правления. При выявлении грубых ошибок и недостатков, при систематическом допущении ошибок, а также при несвоевременном устранении выявленных ошибок и недостатков, руководитель службы внутреннего контроля может дать Председателю Правления рекомендации по совершенствованию системы внутреннего контроля, принятию мер в отношении виновных сотрудников.

10.7. Правление Банка, с учетом изменений во внешней и внутренней ситуациях,

осуществляет постоянных мониторинг системы внутреннего контроля Банка и принимает меры по усилению ее деятельности для обеспечения эффективной работы.

10.8. Мониторинг эффективности системы внутреннего контроля может осуществляться службы внутреннего аудита Банка. В целях мониторинга эффективности системы внутреннего контроля в области противодействия отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, а также подтверждения соответствия внутренних процедур Банка может также проводить независимый внешний аудит. Периодичность такой проверки определяется Банком самостоятельно, при этом частота не может быть реже 1 раза в 2 года.

10.9. Недостатки системы внутреннего контроля, выявленные Службой внутреннего аудита, независимым внешним аудитом или другими контролирующими службами, своевременно доводятся до сведения Председателя Правления Банка. После получения такой информации Председатель Правления принимает меры по своевременному устранению выявленных недостатков.

10.10. Правление Банка с целью усиления, повышения эффективности внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма, обсуждения результатов проверки, проведенной службой внутреннего аудита в отношении выполнения требований законодательства по внутреннему контролю, обязано не реже одного раза в год проводить собрание, при необходимости с приглашением руководителей соответствующих управлений или филиалов.

Приложение № 1
к Правилам внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «Asia Alliance Bank»

ИНФОРМАЦИЯ,
необходимая при идентификации физических лиц

1. Фамилия, имя и отчество.

2. Дата и место рождения.

3. Гражданство.

4. Место постоянного и (или) временного проживания.

5. Реквизиты паспорта или заменяющего его документа: серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ.

6. Персональный идентификационный номер физического лица.(ПИНФЛ)

7. Идентификационный номер налогоплательщика (если имеется).

8. Номер домашнего и мобильного телефона (если имеется).

9. Адрес электронной почты (если имеется).

Приложение № 2
к Правилам внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «Asia Alliance Bank»

ИНФОРМАЦИЯ,
необходимая при идентификации юридических лиц и индивидуальных предпринимателей

1. Информация, необходимая при идентификации юридических лиц:

а) полное, а также сокращенное наименование, если оно указано в свидетельстве о государственной регистрации;

б) информация о государственной регистрации: дата, номер, наименование регистрирующего органа;

в) дата первоначальной регистрации предприятия (или его правопреемника)

г) идентификационный номер налогоплательщика;

д) местонахождение (почтовый адрес);

е) другие данные, указанные в свидетельстве о государственной регистрации;

ж) информация об имеющихся лицензиях на осуществление видов деятельности, подлежащих лицензированию: вид деятельности, номер и дата выдачи лицензии; кем выдана; срок действия;

з) данные об идентификации физических лиц, имеющих право подписи, или физического лица, действующего от имени юридического лица;

и) информация об учредителях (крупных акционерах, участниках) и об их долевых участиях в уставном фонде (капитале) юридического лица;

к) информация о величине зарегистрированного и оплаченного уставного фонда (капитала);

л) информация об органах управления юридического лица (структура и персональный состав органов управления юридического лица);

м) номера телефонов;

н) ВЭБ-сайт и адрес электронной почты (если имеется).

2. Информация, необходимая при идентификации индивидуальных предпринимателей:

а) информация, предусмотренная приложением № 1 к настоящим Правилам;

б) информация о государственной регистрации: дата, номер, наименование регистрирующего органа;

в) место осуществления деятельности;

г) другие данные, указанные в свидетельстве о государственной регистрации;

д) информация об имеющихся свидетельствах и лицензиях на осуществление видов деятельности: вид деятельности, номер, дата выдачи; кем выдана; срок действия;

е) номера телефонов;

ж) ВЭБ-сайт и адрес электронной почты (если имеется).

Приложение № 3
к Правилам внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «Asia Alliance Bank»

ИНФОРМАЦИЯ,
указываемая в анкете клиента

1. Информация, полученная в процессе идентификации клиента, указанная в приложениях №№ 1 и 2 к настоящим Правилам.

2. Информация об уровне риска, включая обоснование оценки риска.

3. Результаты дополнительных мероприятий, проведенных банком при идентификации клиента.

4. Дата начала отношений с клиентом — дата открытия первого банковского счета (вклада) в коммерческом банке.

5. Дата заполнения и внесения изменений в анкету клиента.

6. Фамилия, имя и отчество, должность сотрудника, ответственного за работу с клиентом, в частности, сотрудника, открывшего счет (главного бухгалтера или его заместителя) и утвердившего открытие счета.

7. Подпись сотрудника, заполнившего анкету клиента на бумажном носителе (с указанием фамилии, имени и отчества, должности) и фамилия, имя и отчество, должность сотрудника, заполнившего анкету клиента в электронном виде.

8. Иные данные, определяемые внутренними правилами.

Приложение № 4
к Правилам внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «Asia Alliance Bank»

ASIA ALLIANCE BANK

АНКЕТА БАНКА КОРРЕСПОНДЕНТА
(для стран СНГ)

I. Общие данные */

1.1. Наименование Банка (согласно Устава)			
а) Полное и сокращенное наименование на русском языке: б) Сокращенное наименование на иностранном языке:			
1.2. Организационно - правовая форма			
1.3. Сведения о государственной регистрации			
а) Орган государственной регистрации: б) Дата государственной регистрации: в) Номер государственной регистрации: г) Место государственной регистрации: д) Документ удостоверяющий государственную регистрацию:			
1.4. Идентификационный номер налогоплательщика (ИНН)		**1.6. Коды форм государственного статистического наблюдения**	
		ОКПО	
1.5. Банковские коды		ОКОГУ	
Банковский идентификационный код (БИК)		ОКАТО	
SWIFT		ОКВЭД	
TELEX		ОКФС	
		ОКОПФ	
1.7. Лицензии (разрешения) на осуществление отдельных банковских операций			
а) Вид лицензии: б) Орган выдавший лицензию: в) Дата выдачи лицензии: г) Номер лицензии:			
1.8. Адрес			
а) Юридический адрес: б) Почтовый адрес			
1.9. Контакты			
а) Телефоны: б) Факс:		в) Официальный ВЕБ-сайт: г) Адрес электронной почты:	

*/Все строки анкеты должны быть заполнены, при отсутствии сведений по какой-либо строке, следует указать слова: «сведения отсутствуют».

II. Данные о структуре и положении на рынке

2.1. Информация об основных учредителях/участниках (доля которых 10% и более): наименование, адрес местонахождения **/
2.2. Сведения об органах управления (структура и персональный состав)
2.3. Лицо, которое имеет право действовать от имени Банка без доверенности
2.4 Сведения об уставном капитале
а) Зарегистрировано: б) Оплачено:
2.5.Сведения о дочерних и зависимых компаниях
2.6. Сведения об основных банках корреспондентах
2.7. История, репутация, сектор рынка и конкуренция (например, ссылка на Bankers Almanac)
2.8. Сведения о наименовании внешней аудиторской организации, осуществляющей аудит достоверности бухгалтерской отчетности банка, с указанием даты последней аудиторской проверки
2.9. Наличие у Банка рейтинговой оценки, присвоенной международным рейтинговым агентством (Moody`s Investors Service, Standard&Poor`s или Fitch Ratings)
2.10. Осуществляет ли финансовое учреждение следующие финансовые операции:
- Размещение привлеченных средств от своего имени, на собственных условиях и на собственный риск; ☐ *да* ☐ *нет*
- Открытие корреспондентских счетов в уполномоченных банках своей страны в иностранной валюте и осуществление операций по ним; ☐ *да* ☐ *нет*
- Операции с банковскими металлами на валютном рынке своей страны; ☐ *да* ☐ *нет*
- Организация купли и продажи ценных бумаг по поручительствам клиентов; ☐ *да* ☐ *нет*
- Приобретение права требования на исполнение обязательств в денежной форме за поставленные товары или предоставленные услуги, принимая на себя риск исполнения таких требований и прием платежей (факторинг); ☐ *да* ☐ *нет*

****/** Указать имеются ли среди учредителей и акционеров публичные должностные лица

III. Меры, направленные на противодействие легализации доходов, полученных незаконным путем, и финансированию терроризма

3.1. Перечислите законы и нормативные акты, направленные на противодействие легализации доходов, полученных незаконным путем, и вовлечению банков в незаконные операции, действующие в Вашей стране. Является ли Ваш Банк безусловным исполнителем этих законов?

3.2. Какие нормативные документы регламентируют в Вашем Банке процедуры осуществления комплаенс-контроля, направленного на предотвращение отмыванию доходов, и финансированию терроризма (ПОД/ФТ)? */**
3.3. Наличие и наименование структурного подразделения, выполняющего функции, связанные с ПОД/ФТ
3.4. Сведения об ответственном сотруднике службы комплаенс-контроля
а) Ф.И.О.: б) должность: в) контактный телефон: г) e-mail:
3.5. Применяет ли Ваш банк процедуры контроля в целях противодействия финансированию терроризма? Если да, то какие?
☐ *да* ☐ *нет*
3.6. Применяется ли в Вашем банке принцип «Знай своего клиента» (Идентификация клиента)? Предоставьте, пожалуйста, подробную информацию.
☐ *да* ☐ *нет*
3.7. Применяются ли в филиалах Вашего банка (если таковые имеются) процедуры внутреннего контроля в целях противодействия легализации доходов, полученных незаконным путем?
☐ *да* ☐ *нет*
3.8. Применяются ли процедуры по предотвращению легализации доходов, полученных незаконным путем, в Ваших иностранных отделениях и дочерних компаниях?
☐ *да* ☐ *нет*
3.9. Существует ли в Вашем Банке программа подготовки сотрудников по вопросам рассмотрения противодействия легализации доходов, полученных преступным путем? Предоставьте, пожалуйста, подробную информацию.
☐ *да* ☐ *нет*
3.10. Существует ли в вашем учреждении система отслеживания за счетами и транзакциями для обнаружения подозрительной деятельности? Имеется ли программное обеспечение, если имеется, предоставьте, пожалуйста, информацию.
☐ *да* ☐ *нет*
3.11. Как Вы устанавливаете источник происхождения средств, зачисленных на счет вашего клиента?
3.12. По каким критериям в Вашем Банке осуществляется оценка уровня риска осуществляемой клиентом легализации доходов, полученных незаконным путем?
3.13. Сведения о наличии филиалов и представительств в государствах (на территориях),

которые не участвуют в международном сотрудничестве в сфере ПОД/ФТ
3.14. Поддерживает ли Ваш Банк корреспондентские отношения с банками, зарегистрированных в государствах и на территориях с льготным налоговым режимом (или) не предусматривающих раскрытие и предоставление информации при проведении финансовых операций (т.н. офшорные зоны)? Если да, укажите эти банки-корреспонденты.
☐ *да* ☐ *нет*
3.15. Устанавливает ли Ваш Банк корреспондентские отношения с банками, которые не имеют физического присутствия в какой-либо стране (так называемые « Shell Banks»)?
☐ *да* ☐ *нет*
3.16. Существует ли в вашем учреждении процедура по предотвращению открытия счетов физическим и юридическим лицам, причастных к легализации (отмывание) доходов и к террористической деятельности, находящиеся в «черном списке» списке OFAC/EU/UN? Укажите подробную информацию.
3.17. Проводились ли в отношении Вашего Банка расследования нарушений, связанных с легализацией доходов, полученных от преступной деятельности и финансированию терроризма?
☐ *да* ☐ *нет*
3.18. Имеет ли возможность Ваш Банк предоставить идентификационные данные о клиенте по запросу нашего Банка с целью изучения операции?
☐ *да* ☐ *нет*

***/ Укажите наименование документа, номер и дату его принятия.

Подтверждение: (подписавший подтверждает, что вышеупомянутая анкета содержит достоверную информацию.

Руководитель Банка:

_____

(*Должность*) (подпись) (Ф.И.О.)

Сотрудник комплаенс-контроля:

_____

(*Должность*) (подпись) (Ф.И.О.)

М.П. **Дата: « » 20 г.**

Приложение № 5
к Правилам внутреннего контроля по
противодействию легализации доходов, полученных
от преступной деятельности, и финансированию
терроризма в АКБ «Asia Alliance Bank»

ASIA ALLIANCE BANK

Questionnaire

(to be filled by a partner financial institution)

I. General Information

1.1. Full legal name of financial institution (FI)			
1.2. Legal Form (for example Public Limited Company, Joint Stock Company, Partnership, but this is not exhaustive etc.)			
1.3. Legal address			
1.4. Mailing address			
1.5. Registration/License No		**1.6. Date of registration**	
1.7. Registration body			
1.8. Type of license			
1.9. License number		**1.10. Date of issue of the license**	
1.11. SWIFT, TELEX			
1.12. FI contacts		**1.13. Key contact person**	
Telephone		Name:	
Fax		Title	
Website address		Telephone	
e-mail		e-mail	

II. Ownership, management and regulatory information

2.1. If FI is publicly held, please indicate exchange on which shares are traded:		
2.2. If Institution is privately owned, please list the names of all owners in the table below and their ownership interest (add further rows if necessary)		
Name	Domicile (country, city)	Ownership

		interest (%)

2.3. Supervisory Council

Name	Domicile (country, city)	Main type of activity

2.4. Executive Management / Board of Directors of Institution

Name	Domicile (country, city)	Position

2.5. Have there been any significant changes in ownership (exceeding 25%) over the last five years?

☐*Yes* ☐*No*

If yes, please provide details:

2.6. Please indicate the ultimate beneficial owner(s) of your FI, if any, including personal data (i.e. place and date of birth, domicile).

For the meaning of "Beneficial Owner" please refer to the definition given at the end of this questionnaire.

2.7. Does your Bank have branches, subsidiaries, affiliates and representative offices?

☐*Yes* ☐*No*

If yes, specify them

2.8. Name of your Financial Intelligence Unit (FIU)

2.9. Are your FI subject to external audit activities?

☐*Yes* ☐*No*

If yes, please provide the name of your external auditors. (An external auditor does not mean the Central Bank or Government Body)

III. Anti-Money Laundering and Counter Terrorist Financing

(If you answer "no" to any question, additional information can be supplied at the end of the questionnaire)

A. General AML Policies, Practices and Procedures:	**Yes**	**No**
3.1. Is the AML compliance program approved by the FI's board or a senior committee?	☐	☐
3.2. Does the FI have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework?	☐	☐
3.3. Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?	☐	☐
3.4. In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	☐	☐
3.5. Does the FI have a policy prohibiting accounts/relationships with shell	☐	☐

banks?		
3.6. Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	☐	☐
3.7. Does the FI have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?	☐	☐
3.8. Does the FI have record retention procedures that comply with applicable law?	☐	☐
3.9. Are the FI's AML policies and practices being applied to all branches and subsidiaries of the FI both in the home country and in locations outside of that jurisdiction?	☐	☐
3.10. Has your FI had any regulatory or criminal enforcement actions resulting due to violations of anti-money laundering laws or regulations?	☐	☐
B. Risk Assessment	**Yes**	**No**
3.11. Does the FI have a risk-based assessment of its customer base and their transactions?	☐	☐
3.12. Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	☐	☐
C. Know Your Customer, Due Diligence and Enhanced Due Diligence	**Yes**	**No**
3.13. Has the FI implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?	☐	☐
3.14. Does the FI have a requirement to collect information regarding its customers' business activities?	☐	☐
3.15. Does the FI assess its FI customers' AML policies or practices?	☐	☐
3.16. Does the FI have a process to review and, where appropriate, update customer information relating to high risk client information?	☐	☐
3.17. Does the FI have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?	☐	☐
3.18. Does the FI complete a risk-based assessment to understand the normal and expected transactions of its customers?	☐	☐
3.19. Does your FI ability to provide essential identification data about the client according to the inquiry of the bank respondent in order to examine operations?	☐	☐
D. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds	**Yes**	**No**
3.20. Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	☐	☐
3.21. Where cash transaction reporting is mandatory, does the FI have procedures to identify transactions structured to avoid such obligations?	☐	☐
3.22. Does the FI screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities?	☐	☐
3.23. Does the FI have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?	☐	☐
E. Transaction Monitoring	**Yes**	**No**
3.24. Does the FI have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers checks, money orders, etc?	☐	☐
F. AML Training	**Yes**	**No**
3.25. Does the FI provide AML training to relevant employees that includes: ▪ Identification and reporting of transactions that must be reported to government authorities. ▪ Examples of different forms of money laundering involving the FI's products and services. ▪ Internal policies to prevent money laundering.	☐	☐
3.26. Does the FI retain records of its training sessions including attendance records and relevant training materials used?	☐	☐
3.27. Does the FI communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	☐	☐

3.28. Does the FI employ third parties to carry out some of the functions of the FI?	☐	☐
3.29. If the answer to question 26 is yes, does the FI provide AML training to relevant third parties that includes: ▪ Identification and reporting of transactions that must be reported to government authorities. ▪ Examples of different forms of money laundering involving the FI's products and services. ▪ Internal policies to prevent money laundering.	☐	☐

Space for additional information:
(Please indicate which question the information is referring to.)
.....
.....
.....
.....
.....
.....

I confirm that, to the best of my knowledge, the above information is current, accurate and reflective of my institution's anti-money laundering policies.	
Signature:	
Title:	
Date:	

(Seal)

In this questionnaire the following references are used:

- "Beneficial owner" means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:
  a) in the case of corporate entities:
     (i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;
     (ii) the natural person(s) who otherwise exercises control over the management of a legal entity:
  b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
     (i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;
     (ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
     (iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity.
- "Politically exposed person" means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.
- "Shell banks" means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

Приложение № 6
к Правилам внутреннего контроля по
противодействию легализации доходов, полученных
от преступной деятельности, и финансированию
терроризма в АКБ «Asia Alliance Bank»

Требования, предъявляемые для внесения данных в электронные анкеты клиентов

1. Анкеты клиентов заполняются соответствующими сотрудниками перед осуществлением операции, не позднее даты открытия первого счета.

2. Все ячейки (поля) анкеты, подлежащие к обязательному заполнению, должны быть заполнены полностью, а необязательные ячейки должны быть заполнены полностью по мере возможности. Данные предназначенные для внесения в определенную ячейку, не могут быть записаны в других ячейках.

3. Все сведения записываются на узбекском языке, являющимся государственным языком, если иное не указано в документе, подтверждающем личность (физическим лицам) или документе, подтверждающем государственную регистрацию (юридическим лицам).

4. Наименования клиентов должны быть внесены по в точном соответствии с записями в документе, подтверждающем личность (физическим лицам) или документе, подтверждающем государственную регистрацию (юридическим лицам).

5. Фамилия, имя, отчество физических лиц вносится в записанной в документе, подтверждающем личность (кириллица, латиница и т.п.) и только прописными буквами, если в данном документе не иначе.

6. При внесении наименования юридических лиц сначала записывается наименование, а затем организационно правовая форма и форма собственности, если в документе о государственной регистрации не иначе. Наименование юридических лиц резидентов записываются в кавычках. При записи сокращенного наименования юридических лиц используются следующие аббревиатуры: частное предприятие – ЧП, общество с ограниченной ответственностью – ООО, совместное предприятие – СП, иностранное предприятие – ИП.

Наименование юридических лиц на русском и иностранном языках записываются в точном соответствии с записями в их учредительных документах.

7. При представлении юридическим лицом нескольких документов о государственной регистрации или учредительных документов, вносятся сведения последней из них, которые действительны.

8. Наименование клиента, адреса, и другие данные анкеты должны быть внесены без ошибок, прои этом не используются дополнительные знаки (пробелы, кавычки, тире).

9. Сведение о том, является ли клиент резидентом или нерезидентом необходимо указать безошибочно.

10. Адрес клиента записывается в порядке снижения следующим образом: почтовый индекс, область, город или район, сельский сход граждан, махалля, улица, дом, квартира. При этом каждое наименование отделяется запятым,. используются следующие

аббревиатуры: область – вил., город – ш., район – тум., сельский сход граждан – к.ф.й., улица – кўч.

Адреса иностранных клиентов записываются в соответствии с указанным в документе.

11. Наименования органа выдавшего документ, удостоверяющий личность физических лиц, а также наименования органа осуществившего государственную регистрацию юридических лиц записывается в порядке, указанном в документе, без отделения запятым, при этом аббревиатура не используется. Например: Тошкент шаҳар Шайхонтоҳур тумани ИИБ, Тошкент вилояти Қибрай тумани Ҳокимияти и т.д..

Иностранные органы записываются в соответствии с указанным в документе.

12. При внесении изменений в имеющиеся данные идентификации клиента, работники соответствующих отделов обязаны внести соответствующие изменения в анкету клиента и сообщить об этом сотрудникам Службы внутреннего контроля.

Приложение №7
к Правилам внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ «Asia Alliance Bank»

Службе внутреннего контроля

Извещение

В соответствии с пунктом 64 «Правил внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в коммерческих банках», зарегистрированным 23 мая 2017 года в Министерстве юстиции за № 2886 сообщаю о сомнительной/подозрительной (не нужное зачеркнуть) операции, выявленной в ходе текущей проверки операции клиента:

Дата осуществления операции: _____

Вид документа (операции): _____

Наименование плательщика: _____
(если нерезидент, указывается государство)

Наименование банка плательщика: _____ Код банка: _____

Наименование получателя: _____
(если нерезидент, указывается государство)

Наименование банка получателя: _____ Код банка: _____

Сумма операции: _____
(сумма цифрами и прописью, наименование валюты)

_____

Предмет платежа: _____

_____

Критерий или признак сомнительной/подозрительной операции: _____

_____

Сотрудник представивший сообщение:

Должность _____ _____ Ф.И.О. _____
(подпись)

Дата _____

Принял сообщение:

Должность _____ _____ Ф.И.О. _____
(подпись)

Дата _____

Критерий, присвоенный сотрудником внутреннего контроля:

Вид операции	Кол-во критериев

Приложение № 8
к Правилам внутреннего контроля по
противодействию легализации доходов, полученных
от преступной деятельности, и финансированию
терроризма в АКБ «Asia Alliance Bank»

Журнал учета извещений представленных сотрудниками по сомнительным операциям

(левая сторона)

№	Дата операции	Наименование клиента	Уникальный номер клиента	Наименование и страна корреспондента	Банк корреспондента (по МФО или СВИФТ)	Вид платежа (входящий, исходящий)	Сумма операции и валюта

(правая сторона)

Предмет операции	Дата сообщения	Ф.И.О сообщившего сотрудника	Критерий операции		Работа проведенная по операции	Дата сообщения в Головной банк
			Сомни-тельный	Подозри-тельный		

Приложение №9
к Правилам внутреннего контроля по
противодействию легализации доходов, полученных
от преступной деятельности, и финансированию
терроризма в АКБ «Asia Alliance Bank»

Журнал учета сообщенных представленных в Департамент о подозрительных операциях

(левая сторона)

№	Дата операции	Наименование клиента	Уникальный номер клиента	Наименование и страна корреспондента	Банк корреспондента (по МФО или СВИФТ)	Вид платежа (входящий, исходящий)	Сумма операции и валюта

(правая сторона)

Предмет операции	Дата сообщения	Ф.И.О сообщившего сотрудника	Критерий операции		Работа проведенная по операции	Дата сообщения в Департамент
			Сомни-тельный	Подозри-тельный		

Приложение №10
к Правилам внутреннего контроля по
противодействию легализации доходов, полученных
от преступной деятельности, и финансированию
терроризма в АКБ «Asia Alliance Bank»

Журнал учета поручений (документов) клиентов, по которым прекращены операции

№	Дата операции	Номер и дата документа	Наименование клиента	Наименование и страна корреспондента	Банк корреспондента (по МФО или СВИФТ) или система денежных переводов	Сумма операции и валюта	Предмет операции	Дата прекращения операций	Прим.

Приложение №11
к Правилам внутреннего контроля по противодействию
легализации доходов, полученных от преступной деятельности,
и финансированию терроризма в АКБ «Asia Alliance Bank»

Таблица регистрации снятия наличных с пластиковых карт других банков через терминал «ASIA ALLIANCE BANK»

№	Дата операции	Наименование клиента	Паспорт серия	Номер паспорта	Номер пластиковой карты	Код банка, выпустившего пластиковую карту	Наименование банка, выпустившего пластиковую карту	Сумма операции

Приложение №12
к Правилам внутреннего контроля по противодействию
легализации доходов, полученных от преступной деятельности,
и финансированию терроризма в АКБ «Asia Alliance Bank»

Таблица регистрации платежей за товары и услуги с пластиковых карт других банков через терминал «ASIA ALLIANCE BANK»

№	Дата операции	Наименование клиента	Паспорт серия	Номер паспорта	Номер пластиковой карты	Код банка, выпустившего пластиковую карту	Наименование банка, выпустившего пластиковую карту	Имя получателя	Счет получателя	Код банка получателя	Название банка-получателя	Детал платежа	Сумма операции

Приложение №13
к Правилам внутреннего контроля по противодействию
легализации доходов, полученных от преступной деятельности,
и финансированию терроризма в АКБ «Asia Alliance Bank»

Таблица оформления безналичных расчетов за товары и услуги физическими лицами без открытия лицевого счета (через транзитные счета)

№	Дата операции	Наименование клиента	Паспорт серия	Номер паспорта	Номер счета транзита	Наименование транзитный счет	Имя получателя	Счет получателя	Код банка получателя	Название банка-получателя	Детал платежа	Сумма операции

Приложение №14
к Правилам внутреннего контроля по противодействию
легализации доходов, полученных от преступной деятельности,
и финансированию терроризма в АКБ «Asia Alliance Bank»

Таблица регистрации выявленных подозрительных и подозрительных операций

№	Дата первой операции	Последняя дата операции	Наименование клиента	Код клиента	Наименование корреспондента	Наименование страны Корреспондента	Наименование банка Корреспондента или системы денежного перевода	Код банка Корреспондента	Способ оплаты (входящий/ исходящий)	Сумма операции	Код валюты	Назначение платежа

Критерия		Ф.И.О сотрудника передавшего сосбщения	Дата передачи сообщения в СВК или дата выявления сотрудником СВК	Дата сообщения в СВК Головного офиса	Файл сообщения с Филиала	Код филиала	Дата сообщения в Департамент	Наименование фаила сообщения в Департамент	Номер сообщения в Департамент
Сомнительный	Подозрительный								

Приложение № 15
к Правилам внутреннего контроля по
противодействию легализации доходов, полученных
от преступной деятельности, и финансированию
терроризма в АКБ «Asia Alliance Bank»

ОБЯЗАТЕЛЬСТВО
о соблюдении правил противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма

Я, _____
(отдел, должность, Ф.И.О.)

Ознакомлен с Правилами внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, и финансированию терроризма в АКБ “Asia Alliance Bank”.

Получил достаточные знания о сомнительных и подозрительных операциях, а также клиентах и операциях, отнесенных к категории с высокой степенью риска, определенных правилами.

Обязуюсь впредь выполнять следующие функции, предусмотренные в указанных правилах:

- ☐ в установленном порядке осуществлять надлежащую проверку клиента;
- ☐ в случае выявление сомнительных и подозрительных операций, немедленно письменно сообщать об этом управлению внутреннего контроля и непосредственному руководителю;
- ☐ при обращении к сотруднику, непосредственно обслуживающему клиента, о предоставлении дополнительных сведений согласно поручению сотрудника управления внутреннего контроля, в установленном порядке обратиться к клиенту и довести полученную информацию Управлению внутреннего контроля.
- ☐ знать о государствах, не участвующих в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма и оффшорных зонах;
- ☐ повышать знания и навыки в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма. Участвовать в организуемых Банком учебах по данной тематике.

_____	_____	_____
(Ф.И.О.)	(подпись)	(дата)