



П Р А В И Л А
внутреннего контроля АО "АРЕХ BANK" по противодействию
легализации доходов, полученных от преступной деятельности,
финансированию терроризма и финансированию распространения
оружия массового уничтожения

Лист регистрации изменений

№ п/н	Номера листов (страниц)				Всего листов (страниц) В документе	№ изменения	Подпись	Дата
	Измененных	Замененных	Новых	Изъятых				
1	2	3	4	5	6	7	8	9

Содержание:

Лист регистрации изменений

- 1. Общие положения**
- 2. Цели, основные задачи и функции системы внутреннего контроля по ПОД/ФТ/ФРОМУ**
- 3. Структура системы внутреннего контроля по ПОД/ФТ/ФРОМУ**
- 4. Правила надлежащей проверки клиентов, в том числе идентификации клиентов и бенефициарных собственников клиентов, а также осуществления постоянного мониторинга за операциями клиентов**
- 5. Порядок установления деловых отношений с публичными должностными лицами, членами их семей и лицами, близкими к публичным должностным лицам и осуществления углубленного мониторинга ими проводимых операций**
- 6. Требования к установлению и осуществлению отношений с банками-нерезидентами и системами международных денежных переводов, а также меры, принимаемые в случае выявления денежных переводов в иностранной валюте, не имеющих требуемой информации**
- 7. Критерии и признаки сомнительных и подозрительных операций**
- 8. Порядок выявления и безотлагательного приостановления операций лиц, включенных в Перечень, замораживания денежных средств или иного имущества указанных лиц, а также направления их обращений по предоставлению доступа к замороженным денежным средствам или иному имуществу**
- 9. Порядок осуществления мер по изучению, анализу, выявлению, оценке, мониторингу, управлению, снижению и документированию риска**
- 10. Выявление сомнительных и подозрительных операций, а также подготовка и направление сообщений о подозрительных операциях в специально уполномоченный государственный орган**
- 11. Порядок направления запросов специально уполномоченным государственным органом**
- 12. Оформление, хранение, обеспечение конфиденциальности информации и документов**
- 13. Квалификационные требования к подготовке и обучению кадров**
- 14. Ответственность сотрудников Департамента по ПОД/ФТ/ФРОМУ и санкционному комплаенсу и других подразделений**
- 15. Заключительные положения**

I. Общие положения

1.1 Настоящие Правила разработаны в соответствии с Законами Республики Узбекистан «О Центральном банке Республики Узбекистан», «О банках и банковской деятельности», «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения» (далее-ПОД/ФТ/ФРОМУ), «О банковской тайне», 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, Правилами внутреннего контроля по ПОД/ФТ/ФРОМУ в коммерческих банках, Правилами открытия, ведения и закрытия корреспондентских счетов АО "APEX BANK", Методическими рекомендациями по осуществлению операторами платежных систем, операторами электронных денег, платежными организациями комплексного анализа по выявлению подозрительных операций, связанных с легализацией доходов, полученных от преступной деятельности, финансированием терроризма и финансированием распространения оружия массового уничтожения, Положения АО "APEX BANK" О порядке цифровой идентификации клиентов и определяют порядок организации, а также осуществления внутреннего контроля в банке, в целях создания эффективной системы по ПОД/ФТ/ФРОМУ.

1.2 В настоящих Правилах используются следующие основные понятия:

Банк — акционерное общество "APEX BANK";

бенефициарный собственник — лицо, которое в конечном итоге владеет правами собственности или реально контролирует клиента, и в интересах которого совершается операция;

внутренний контроль — деятельность 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;

государства, не участвующие в международном сотрудничестве в сфере ПОД/ФТ/ФРОМУ — 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 ПОД/ФТ/ФРОМУ имеет стратегические недостатки;

дистанционные услуги — банковские услуги, предоставляемые по проведению

операций с использованием программ, дающих возможность осуществления операций без явки клиента в Банк;

идентификация бенефициарного собственника клиента — определение собственника юридического лица, в том числе лица, контролирующего клиента, путем изучения структуры собственности и управления на основании учредительных документов (устава и (или) учредительного договора, положения и других, равносильных документов);

идентификация клиента — определение 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;

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);

клиент — физическое или юридическое лицо, обратившееся в Банк с поручением (заявлением, ходатайством) об осуществлении операции;

компетентные органы Республики Узбекистан — Служба государственной безопасности, Министерство внутренних дел, Генеральная прокуратура и Государственный комитет промышленной безопасности Республики Узбекистан;

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;

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 предоставленным сведениям о таком клиенте и его деятельности;

операция — вид деятельности, определенной Законом Республики Узбекистан «О банках и банковской деятельности» как банковская операция (в том числе, открытие и ведение счетов физических или юридических лиц, осуществление расчетов по счетам, привлечение вкладов, предоставление кредитов, лизинга и других услуг, по сути являющимися кредитами, покупка у юридических и физических лиц и продажа им иностранной валюты в наличной и безналичной формах, выдача гарантий за третьих лиц, выпуск, покупка, продажа, учет и хранение ценных бумаг, предоставление в аренду физическим и юридическим лицам специальных помещений или находящихся в них сейфов для хранения документов и иных ценностей и другие);

ответственное подразделение — структурное подразделение Банка (департамент, управление, отдел, сектор, офис продаж и др., кроме Департамента по ПОД/ФТ/ФРОМУ и санкционному комплаенсу и его подразделений), ответственное за выполнение функций, в процесс которых данными Правилами внедрены требования в целях осуществления внутреннего контроля;

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

Перечень — перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, формируемый специально уполномоченным государственным органом 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;

санкционные перечни Совета Безопасности ООН — перечни физических и юридических лиц, причастных к террористической деятельности или распространению оружия массового уничтожения, в отношении которых предусмотрено применение санкций, составляемые Советом Безопасности ООН и его комитетами, в том числе комитетом Совета Безопасности ООН, созданным на основании резолюций 1267, 1989 и 2253 по ИГИЛ (ДАИШ) и «Аль-Каида», а также комитетами, созданными на основании резолюций 1988 по организации «Талибан» и 1718 по Корейской Народно-Демократической Республике;

соответствующие резолюции Совета Безопасности ООН — резолюции, принятые Советом Безопасности ООН, направленные на противодействие терроризму (резолюции 1267 (1999), 1333 (2000), 1363 (2001), 1373 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), 1989 (2011), 2161 (2014), 2170 (2014), 2178 (2014), 2253 (2015), 2368 (2017) и резолюции, принятые в их развитие) или распространению оружия массового уничтожения (1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), 1929 (2010), 2087 (2013), 2094 (2013), 2231 (2015), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017),

2375 (2017), 2397 (2017) и резолюции, принятые в их развитие);

подозрительная операция — операция, находящаяся в процессе подготовки, совершения или уже совершенная, в отношении которой 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;

сомнительная операция — операция, в отношении которой в процессе проведения внутреннего контроля возникло основание полагать об осуществлении данной операции с целью легализации доходов, полученных от преступной деятельности, финансирования терроризма и (или) финансирования распространения оружия массового уничтожения, до принятия решения о включении (не включении) ее в категорию подозрительной операции;

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

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);

работник — лицо, на которого в соответствии с заключенным с ним трудовым договором и внутренними документами Банка возложены функции по оформлению, одобрению, утверждению и проведению банковских операций, независимо от занимаемой им должности и местом осуществления деятельности (здание Банка, офис продаж и другие виды пунктов обслуживания, находящиеся за пределами здания Банка), в том числе, непосредственно обслуживающее клиентов;

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

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

система внутреннего контроля по ПОД/ФТ/ФРОМУ — совокупность организационной структуры, методик и процедур, направленных на соблюдение требований законодательства в сфере противодействия легализации доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения;

Служба внутреннего контроля — Департамент по ПОД/ФТ/ФРОМУ и санкционному комплаенсу Банка ответственный за управление системы внутреннего контроля Банка по ПОД/ФТ/ФРОМУ и санкционному комплаенсу;

Электронный кошелек - программное обеспечение системы электронных денег, микропроцессор (чип), программно-техническое средство, в котором хранятся электронные деньги, и обеспечивается доступ к ним;

Аккаунт - учетная запись в мобильном приложении, которая включает в себя совокупность информации о клиенте;

сотрудники Службы внутреннего контроля — Директор и работники Департамента по ПОД/ФТ/ФРОМУ и санкционному комплаенсу Банка;

специально уполномоченный государственный орган (далее—СУГО) — Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан (государственный орган по вопросам противодействия легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения, определяемый в соответствии с законодательством);

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";

участники операции — клиенты, их представители, а также партнеры клиента участвующие в операции.

II. Цели, основные задачи и функции системы внутреннего контроля

2.1 Целями системы внутреннего контроля Банка являются:

- 1) эффективное выявление и пресечение операций, направленных на легализацию доходов, полученных от преступной деятельности, финансирование терроризма и распространение оружия массового уничтожения;
- 2) недопущение умышленного или неумышленного вовлечения Банка в преступную деятельность, проникновения преступного капитала в его уставный фонд (капитал), а также проникновения преступных лиц в управление Банком;
- 3) выявление, оценка, документальное фиксирование и снижение рисков;
- 4) обеспечение Банком неукоснительного соблюдения требований законодательства Республики Узбекистан о ПОД/ФТ/ФРОМУ.

2.2 Основными задачами системы внутреннего контроля Банка, независимо от того действуют ли он прямо или через платежных агентов и (или) платежных субагентов, являются:

- 1) принятие соответствующих мер по выявлению и оценке, документальному

фиксированию и снижению своих рисков;

2) осуществление процедур идентификации и мер по надлежащей проверке клиентов, в том числе верификации и регулярного обновления данных о клиенте и их бенефициарных собственниках;

3) идентификация бенефициарных собственников, принятие доступных мер по проверке их личности и определению источников денежных средств или иного имущества, используемого в осуществлении операции;

4) осуществление углубленного мониторинга операций, проводимых публичными должностными лицами, членами их семей и лицами, близкими к публичным должностным лицам;

5) выявление сомнительных и подозрительных операций в порядке, установленном законодательством Республики Узбекистан и настоящими Правилами;

6) своевременное предоставление в СУГО информации (документов) о подозрительных операциях, выявленных в ходе осуществления внутреннего контроля;

7) выявление среди участников операции лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, путем сверки с Перечнем;

8) безотлагательное приостановление операции, за исключением операций по зачислению денежных средств, поступивших на счет юридического или физического лица, и (или) замораживание денежных средств или иного имущества лиц, включенных в Перечень, без их предварительного уведомления;

9) обеспечение конфиденциальности сведений, связанных с ПОД/ФТ/ФРОМУ;

10) обеспечение хранения информации об операциях, а также идентификационных данных и материалов по надлежащей проверке клиентов в течение сроков, установленных законодательством Республики Узбекистан;

11) оперативное и систематическое обеспечение руководства Банка достоверной информацией и материалами, необходимыми для принятия соответствующих решений;

12) формирование базы данных об осуществлении или попытках осуществления подозрительных операций, лицах (руководителях, учредителях, акционерах, являющихся владельцами не менее чем десяти процентов акций общества, участниках), связанных с клиентами, осуществившими подозрительные операции, а также взаимобмен такой информацией с другими коммерческими банками и государственными органами в соответствии с законодательством Республики Узбекистан;

13) изучение системы внутреннего контроля иностранных банков при установлении с ними корреспондентских отношений;

14) применение необходимых мер в целях обращения особого внимания пресечению угрозы использования услуг Банка для совершения правонарушения, в частности, легализации доходов, полученных от преступной деятельности, финансирования терроризма и (или) финансирования распространения оружия массового уничтожения, с помощью новейших технологий, повышающих степень анонимности операций;

15) выявление по запросам в клиентской базе лиц, связанных с легализацией доходов, полученных от преступной деятельности, финансированием террористической деятельности и (или) финансированием распространения оружия массового уничтожения.

2.3 Для достижения целей и задач системы внутреннего контроля Служба внутреннего контроля осуществляет функции по:

1) принятию мер, предусмотренных законодательством, настоящими Правилами, внутренними документами, для пресечения угрозы использования услуг Банка для легализации доходов, полученных от преступной деятельности, финансирования терроризма и (или) финансирования распространения оружия массового уничтожения;

2) осуществлению мониторинга соблюдения Банком требований законодательства и внутренних документов о ПОД/ФТ/ФРОМУ;

3) подготовке и внесению на рассмотрение руководства предложения об устранении выявленных недостатков и правонарушений в деятельности Банка в части несоблюдения требований законодательства и внутренних документов о ПОД/ФТ/ФРОМУ;

4) осуществлению мониторинга устранения ошибок и недостатков в организации и функционировании системы внутреннего контроля, обнаруженных в ходе проверок полномочными представителями Центрального банка Республики Узбекистан (далее — Центральный банк), работниками Службы внутреннего аудита банка, внешними аудиторами и сотрудниками СУГО;

5) взаимодействию с Центральным банком и СУГО по вопросам организации внутреннего контроля, предупреждения и устранения нарушений работниками требований законодательства, настоящих Правил и внутренних документов.

III. Структура системы внутреннего контроля по ПОД/ФТ/ФРОМУ

3.1 Система внутреннего контроля по ПОД/ФТ/ФРОМУ Банка организуется с учетом особенностей функционирования банка, основных направлений его деятельности, агентской, субагентской, клиентской базы и уровня рисков, связанных с клиентами и их операциями.

3.2 Структура системы внутреннего контроля по ПОД/ФТ/ФРОМУ Банка определяется решением Наблюдательного Совета банка и должна пересматриваться с учетом выявленных рисков и их оценки, а также в соответствии с требованиями Центрального банка Республики Узбекистан.

3.3 Структура системы внутреннего контроля по ПОД/ФТ/ФРОМУ Банка включает в себя Службу внутреннего контроля, Департамент внутреннего контроля и комплаенс и другие ответственные подразделения Банка, вовлеченные в процесс достижения целей и выполнения задач, определенные настоящими Правилами.

IV. Правила надлежащей проверки клиентов, в том числе идентификации клиентов и бенефициарных собственников клиентов, а также осуществления постоянного мониторинга за операциями клиентов

4.1 Банк обязан самостоятельно принимать меры по надлежащей проверке клиентов в следующих случаях:

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

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

б) при обращении физического лица с заявлением на получение банковской пластиковой карты;

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

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

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

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

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

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

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

г) при совершении или получении денежных переводов, предусмотренных пунктом 6.12 настоящих Правил;

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

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

4.2 Платежные агенты и платежные субагенты могут проводить проверку личности и идентификацию клиентов в целях применения мер по надлежащей проверке клиента, при соблюдении требований законодательства о ПОД/ФТ/ФРОМУ, в случаях если это предусмотрено агентским и (или) субагентским договором.

4.3 Меры по надлежащей проверке клиента, принимаемые Банком, обязательно включают:

- 1) проверку личности и идентификацию клиента, полномочий клиента и лиц, от имени которых он действует на основании соответствующих документов;
- 2) идентификацию бенефициарного собственника клиента;
- 3) изучение цели и характера деловых отношений или запланированных операций;
- 4) идентификацию, проверку личности и полномочий лица, действующего от имени клиента, на основании соответствующих документов;
- 5) 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.

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

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

4.4 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 подпункте 1) пункта 4.3 настоящих Правил могут быть проведены Центрами государственных услуг (далее — регистрирующий орган) Республики Узбекистан и Банк может доверять результатам проведенных мер. При этом работники должны удостовериться:

- 1) в возможности незамедлительного получения необходимой информации по

мерам надлежащей проверке клиента через автоматизированную систему государственной регистрации и постановки на учет субъектов предпринимательства;

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

В случае невыполнения требований, указанных в подпунктах 1) и 2) настоящего пункта, работники самостоятельно проводят меры по надлежащей проверке клиента.

При проведении мер по надлежащей проверке клиентов регистрирующим органом решение о вступлении в деловые отношения с клиентом работники принимают самостоятельно, исходя от риска. При этом в оферте договора банковского счета должно быть указано право проведения Банком мер по надлежащей проверке клиентов.

4.5 Банк может доверять результатам надлежащей проверки клиента, проведенной третьими сторонами, по мерам надлежащей проверки, указанным в абзацах а) и б) подпункта 1) пункта 4.1 настоящих Правил. В таких случаях конечную ответственность по надлежащей проверке клиента несет Банк. При этом Банк должен 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 руководствуется внутренними правилами по ПОД/ФТ/ФРОМУ.

В случае несоблюдения одного из требований, предусмотренных в абзацах втором – четвертом настоящего пункта, Банк самостоятельно принимает меры по надлежащей проверке клиентов.

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

Банк должен оговорить о возможности принятия мер по надлежащей проверке клиентов в договоре и/или в договоре оферте.

Банк так же может осуществлять и цифровую идентификацию своих клиентов в порядке, предусмотренном в внутреннем нормативном документе.

4.6 Усиленные меры по надлежащей проверке клиентов включают следующие:

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

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

3) изучение целей, запланированных или проведенных данным клиентом операций;

4) 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 СУГО и отказаться от вступления в деловые отношения с таким клиентом или от проведения операций такого клиента.

4.7 Идентификация клиента и бенефициарного собственника клиента осуществляется работниками на основе информации, предусмотренной приложениями 1 и 2 к настоящим Правилам, а также документов, являющихся основанием совершения операций и иных сделок, и другой необходимой информации.

4.8 Идентификация клиента — физического лица Банком 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 должен ознакомиться с оригиналом такого документа;

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

4.9 При применении мер надлежащей проверки клиентов в отношении юридических лиц и индивидуальных предпринимателей Банк должен получить у них:

1) соответствующие документы о государственной регистрации юридических лиц и индивидуальных предпринимателей;

2) сведения о руководителях, а также сведения, указанные в учредительных документах юридических лиц.

Получение данных сведений осуществляется через автоматизированную систему государственной регистрации и постановки на учёт субъектов предпринимательства, а в случае невозможности получения данных из этой системы - непосредственно от клиента.

4.10 В процессе надлежащей проверки юридических лиц Банк должен идентифицировать физическое лицо-бенефициарного собственника клиента, являющегося в конечном итоге собственником клиента или контролирующего клиента, применять обоснованные меры по проверке личности бенефициарного собственника, используя сведения, полученные из надёжного источника, в том числе изучения:

1) структуры собственности и управления клиента;

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

3) 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 Банком, Банк должен идентифицировать лицо, занимающее высокую руководящую должность, и принять обоснованные меры по проверке его личности.

4.11 Если клиентом или бенефициарным собственником клиента является юридическое лицо, на которое распространяются требования нормативно-правовых актов Республики Узбекистан 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.

4.12 Работник в целях более тщательного изучения клиента — юридического лица должен уделять особое внимание:

- 1) составу учредителей (акционеров, являющихся владельцами не менее чем десяти процентов акций общества, участников) клиента, определению лиц, владеющих долей свыше 10 процентов уставного фонда (капитала) клиента;
- 2) структуре органов управления клиента и их полномочиям;
- 3) размеру зарегистрированного уставного фонда (капитала) клиента.

4.13 К иностранным структурам без образования юридического лица применяются требования, установленные настоящими Правилами к юридическим лицам.

4.14 Все документы, позволяющие идентифицировать клиента и иных участников операции, должны быть действительными на дату их предъявления.

4.15 Работники, при наличии подозрений в достоверности полученной(ых) информации (документов), должны принять меры по проверке (верификации) этой (этих) информации (документов). В таком случае, Банк вправе обратиться в соответствующие организации с запросом для выяснения достоверности (подлинности) информации (документов) о клиентах.

4.16 Банк должен применять меры надлежащей проверки в отношении имеющих клиентов с учётом 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.

4.17 Повторная идентификация клиента и бенефициарного собственника работниками должна проводиться в случаях возникновения сомнения в достоверности информации, полученной в результате предыдущей идентификации.

4.18 При идентификации клиента и бенефициарного собственника клиента, в том

числе, когда он действует через своих платежных агентов и (или) платежных субагентов, работники Банка обязаны, сверять полученную информацию с Перечнем, а также со списком государств, не участвующих в международном сотрудничестве в области ПОД/ФТ/ФРОМУ, формируемыми и предоставляемыми коммерческим банкам СУГО в установленном законодательством порядке.

В случае выявления в ходе идентификации клиента и бенефициарного собственника клиента лиц, включенных в Перечень, работник должен принять меры, указанные в главе 8 настоящих Правил.

4.19 Банк вправе отказать клиенту в осуществлении операций в случае:

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

2) предоставления заведомо недостоверных документов или непредставления документов, запрашиваемых в соответствии с законодательством Республики Узбекистан и настоящими Правилами;

3) в иных случаях, предусмотренных законодательством Республики Узбекистан и настоящими Правилами.

4.20 Ответственным подразделениям и работникам запрещается:

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

2) открывать счета на явно вымышленные имена, не подтвержденные документально;

3) открывать счета без личного присутствия лица, открывающего счет, либо его уполномоченного представителя за исключением случаев, когда работник 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 Банком на основании биометрических данных, а также Банк доверяет результатам надлежащей проверки клиентов, проведенной третьей стороной;

4) выпускать ценные бумаги и другие финансовые инструменты на предъявителя;

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

6) оформлять, одобрять, утверждать и проводить операции без сверки идентификационных данных клиента и других участников операции с Перечнем, в том числе, когда одной из сторон операции является Банк;

7) предоставлять доступ прямо или опосредованно к денежным средствам или иному имуществу, материальным ресурсам, финансовым и другим услугам лицам, включенным в Перечень, а также лицам, действующим по их поручению, в том числе, когда одной из сторон операции является Банк, кроме случая, указанного в пункте 8.13

настоящих Правил;

4.21 Банк незамедлительно сообщает в СУГО о связанных с формированием источников денежных средств или иного имущества и запланированных операциях, одновременно имеющих критерии, приведенные в пункте 7.2 настоящих Правил, и проводит такие операции в течение не более трех рабочих дней после осуществления полного анализа в целях выявления уровня риска их взаимосвязанности.

V. Порядок установления деловых отношений с публичными должностными лицами, членами их семей и лицами, близкими к публичным должностным лицам и осуществления углубленного мониторинга ими проводимых операций

5.1 Помимо применения мер по надлежащей проверке клиента в соответствии с требованиями Главы 4 настоящих Правил, в отношении публичных должностных лиц и их близких родственников, выступающих в качестве клиента или бенефициарного собственника клиента, работники должны:

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

2) устанавливать или продолжать для существующих клиентов деловые отношения с публичным должностным лицом только с разрешения Председателя Правления Банка или его уполномоченного заместителя;

3) осуществлять постоянный углубленный мониторинг деловых отношений, в том числе путем увеличения количества и частоты проверок операций клиента, проводимых с целью выявления сомнительных или подозрительных операций.

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

5.2 Документы и сведения, получаемые для открытия счета, в том числе в целях надлежащей проверки клиента, должны быть проанализированы работниками на предмет наличия данных, указывающих на принадлежность клиента или его бенефициарного собственника к категории публичных должностных лиц или их близких родственников.

5.3 Работники при необходимости вправе обращаться в Службу внутреннего контроля за получением дополнительной информации из коммерческих баз данных. В свою очередь, Служба внутреннего контроля должна принять незамедлительные меры для поиска необходимой информации по запросу работника.

VI. Требования к установлению и осуществлению отношений с банками-нерезидентами и системами международных денежных переводов, а также

**меры, принимаемые в случае выявления денежных переводов в
иностранной валюте, не имеющих требуемой информации**

6.1 При установлении и осуществлении корреспондентских отношений с банком-нерезидентом, помимо идентификации банка-нерезидента, ответственному подразделению необходимо:

- 1) собрать информацию о банке-нерезиденте для того, чтобы получить полное представление о характере его деловой деятельности;
- 2) 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;
- 3) оценивать применяемые банком-нерезидентом меры по ПОД/ФТ/ФРОМУ;
- 4) 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;
- 5) сохранять всю информацию об электронном переводе при установлении отношений с другими банками в целях осуществления транзитных переводов;
- 6) убедиться в том, что банки-нерезиденты, с которыми устанавливаются корреспондентские отношения, применяют международные стандарты ПОД/ФТ/ФРОМУ.
- 7) обеспечить четкое и полное распределение обязанностей между корреспондентами.

6.2 Решение об установлении корреспондентских отношений с банком-нерезидентом принимается Правлением Банка по инициативе ответственного подразделения.

6.3 Если банк выступает 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, он должен хранить запись всей информации, полученной от отправлявшего финансового учреждения или другого транзитного финансового учреждения, не менее пяти лет.

6.4 При продолжении корреспондентских отношений с банками-нерезидентами, расположенными на территории государств, не участвующих в международном сотрудничестве в области ПОД/ФТ/ФРОМУ, или их дочерними банками, филиалами и представительствами ответственное подразделение должно проявлять особое внимание всем осуществляемым с ними операциям.

Ответственное подразделение:

1) обязано 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;

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

3) должно 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.

6.5 При установлении и осуществлении отношений с компаниями, предоставляющими услуги по международным денежным переводам (далее — системы международных денежных переводов), помимо идентификации системы международных денежных переводов, ответственное подразделение должно:

1) собрать информацию о системы международных денежных переводов для того, чтобы получить полное представление о характере его деловой деятельности;

2) определить на основе открытой информации репутацию, в том числе проводились ли в отношении данной системы международных денежных переводов расследования нарушений, связанных с легализацией доходов, полученных от преступной деятельности, финансированием терроризма и финансированием распространения оружия массового уничтожения;

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

4) 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;

5) сохранять всю информацию об электронном переводе при установлении отношений с другими банками в целях осуществления транзитных переводов.

6) обеспечить четкое и полное распределение обязанностей между корреспондентами.

6.6 Решение об установлении отношений в части использования систем международных денежных переводов, принимается Правлением Банка.

6.7 Сведения о Банке, персональные данные членов Наблюдательного совета

Банка, членов Правления, других работников и бенефициарных собственников Банка, как отдельно, так и в рамках комплексного запроса, предоставляются банкам-корреспондентам/контрагентам при условии наличия/заключения с ними соглашений о конфиденциальности, обеспечивающих сохранность и конфиденциальность персональных данных.

В случае отсутствия соглашения о конфиденциальности и/или невозможности заключения такого соглашения, сведения о Банке и персональные данные лиц, указанных в вышестоящем пункте, предоставляются с согласия члена Правления, курирующего подразделение, ответственное за предоставление сведений о Банке в рамках соответствующего запроса от банка-корреспондента/контрагента. Таким согласием может быть виза члена Правления на Анкете по ПОД/ФТ, вопроснике КУС, либо на служебной записке, направляемой ответственным подразделением в Службу внутреннего контроля о необходимости предоставления персональных данных или копий паспортов и иных документов, содержащих персональные данные членов Наблюдательного совета, членов Правления, других работников и бенефициарных собственников Банка.

6.8 Ответственное подразделение должно вести учет подразделений (платежных агентов, платежных субагентов, пунктов, отделов и т.п.), предоставляющих клиентам услуги по международным денежным переводам, в том числе через системы международных денежных переводов, и работников этих подразделений.

6.9 Работники, предоставляющие услуги по международным денежным переводам должны:

1) осуществлять операции по денежным переводам (выплата или отправка) после надлежащей проверки клиентов — физических лиц в порядке, установленном настоящими Правилами;

2) обеспечить полноту, точность и своевременность заполнения данных (информацию), предусмотренных в соответствующих модулях автоматизированной банковской системы, а также в программном обеспечении систем международных денежных переводов;

3) обеспечить сопровождение 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, а 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);

4) принимать обоснованные и доступные меры по выявлению международных денежных переводов, не имеющих требуемой информации;

5) отказать в исполнении операции по международным денежным переводам

(выплата и отправление) в случаях отсутствия возможности надлежащей проверки клиента и требуемой информации;

б) направить письменное сообщение в Службу внутреннего контроля в случае отказа в исполнении операции по международным денежным переводам в связи с отсутствием возможности осуществления надлежащей проверки клиента и требуемой информации в день отказа от исполнения операции по форме, согласно Приложению 5 к настоящим Правилам.

6.10 Ответственное подразделение Банка, на которое возложены функции организации и контроля осуществления международных денежных переводов должна:

1) до 10 числа каждого календарного месяца осуществлять проверку отправленных и поступивших международных денежных переводов на предмет отсутствия минимальной информации за прошедший месяц;

2) принять меры по получению отсутствующей минимальной информации (смотреть в пункте 6.11 в подпунктах 1), 2), путем направления соответствующим системам международных денежных переводов и корреспондентам – банкам-нерезидентам требований;

3) хранить переписки с корреспондентами – банками-нерезидентами и системами международных денежных переводов, а также сведения и документы, полученные в рамках исполнения требований настоящего пункта в сроки, установленные законодательством Республики Узбекистан и настоящими Правилами.

6.11 Банк должен иметь возможность получения дополнительной информации об отправителях и получателях денежных средств в течение трех рабочих дней от корреспондентов банков-нерезидентов и систем международных денежных переводов в соответствии с составленными с ними договорами.

В случае отсутствия такой возможности Правление Банка должно рассмотреть вопрос расторжения договора с такими системами международных денежных переводов.

Ответственные подразделение должны:

1) 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;

2) требовать от банков-нерезидентов и систем международных денежных переводов предоставления минимальной информации (наименование отправителя; серия и номер документа, удостоверяющего личность; адрес отправителя или государственный идентификационный номер либо идентификационный номер отправителя; дату и место рождения; номер счета отправителя или уникальный номер операции) об отправителях денежных средств, сумма которых равна или превышает 50-кратный размер базовой расчетной величины;

3) принять во внимание всю информацию, полученную как от отправляющей

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

4) в случае необходимости пересмотреть уровень риска;

5) рассмотреть вопрос о направлении сообщения в СУГО;

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

6.12 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, как предписано для международных денежных переводов, кроме случаев, когда полная информация об отправителе может быть доступна получающему коммерческому банку с помощью других источников. В этом случае отправляющему коммерческому банку достаточно включать 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.

Банк должен 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).

6.13 В случае, когда Банк выступает в качестве посредника (транзитного банка) в денежном переводе, который совершается с использованием корреспондентских счетов, открытых в Банке для других банков-резидентов или банков-нерезидентов, то ответственное подразделение должно:

1) обеспечивать передачу и хранение не менее пяти лет всей информации об отправителе и получателе, сопровождающей электронный перевод, вместе с переводом;

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

3) осуществлять операции по денежным переводам только при наличии требуемой информации;

4) не осуществлять (отклонить либо отказать) исходящий или входящий денежный перевод в случае отсутствия требуемой информации;

5) рассмотреть вопрос о направлении сообщения в СУГО в случае выявления международных денежных переводов, не имеющих требуемой информации о получателе и (или) отправителе;

6) пересмотреть уровень риска.

6.14 Банку запрещается:

- 1) устанавливать и продолжать отношения с банками-нерезидентами, не имеющими на территориях государств, в которых они зарегистрированы, физического присутствия и постоянно действующих органов управления;
- 2) создавать дочерние банки, филиалы или представительства Банка на территории государств, не участвующих в международном сотрудничестве в области ПОД/ФТ/ФРОМУ.

6.15 При наличии информации о нарушении банком-нерезидентом требований международных стандартов по ПОД/ФТ/ФРОМУ, Правление Банка должно рассмотреть вопрос о принятии соответствующих мер, вплоть до прекращения сотрудничества с данным банком-корреспондентом.

VII. Критерии и признаки сомнительных и подозрительных операций

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

- 1) операции или клиенту, ее осуществляющему присвоен высокий уровень риска;
- 2) систематически (например, 3 и более раза в течении одного года) 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 сомнения 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 Банком;
- 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 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 базовой расчетной величины, 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;

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 расчетной 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 расчетной величины;

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

21) другие операции, не имеющие критериев и признаков, предусмотренных в Правилах внутреннего контроля (№2886 от 23.05.2017г) и в данном пункте, в отношении которых имеются подозрения в причастности к легализации доходов, полученных от преступной деятельности, и (или) финансированию терроризма, например:

а) операции, связанные с крупными транзитными операциями или обналичиванием либо конверсией на иностранную валюту;

поступление на карту крупных размеров денежных средств с одного или нескольких карт, электронных кошельков, а также со счетов юридических лиц или индивидуальных предпринимателей; перевод на одну или на множество карт крупных денежных средств; обналичивание крупных средств через банкоматы, а также списание средств через терминалы, конверсия на иностранную валюту через мобильные приложения;

б) операции, связанные с незаконной торговлей, уклонением от уплаты налогов:

систематическое поступление средств с множественных карт, при этом количество транзакции и суммы переводов могут быть разными; поступившая сумма в основном может быть обналичена через банкоматы, сконвертирована на иностранную валюту через мобильные приложения, с дальнейшим обналичиванием, кроме того средства могут переведены на другую карту для расчета за товары;

в) операции, связанные с платформами онлайн-тотализаторов:

систематические поступления на карту малых сумм, в большинстве случаев одинаковых сумм от множества карт и несколькими транзакциями; часть поступивших средств может быть возвращена в более крупных размерах нескольким картам (потенциальная выигрышная сумма), часть средств может использована для иностранных электронных денег (Webmoney, Qiwi и т.д.) через мобильные приложения, часть средств может быть переведена на другие карты (потенциальные владельцы платформы) или может быть обналичена;

г) операции, связанные с мошенничеством:

открытие нового аккаунта, в дальнейшем на данный аккаунт прикрепляется несколько карт, в том числе карта пострадавшего, посредством смс-кода. В дальнейшем списанные средства с карты пострадавшего по цепочке переводится на другие карты и в конце средства обмениваются на зарубежные электронные деньги или конвертируются на иностранную валюту;

д) операции, связанные с купле-продажей крипто-валют:

систематические поступления на карту средств, которые в дальнейшем переводятся на электронные кошельки иностранных платежных систем, для пополнения счетов в крипто-биржах;

е) и другие подозрительные операции;

7.2 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 ПОД/ФТ/ФРОМУ;

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, одновременно или многократно в течение срока, не

превышающего 1 месяцев;

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 Правилах внутреннего контроля (№2886 от 23.05.2017г) и в данном пункте, в отношении которых 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 СУГО);

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

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, одновременно или многократно в течение срока, не превышающего одного месяца.

15) перевод клиентом денежных средств с банковской карты через мобильное приложение на одну (один) или несколько банковских карт или электронных кошельков, одновременно или многократно в течение срока, не превышающего 30 дней, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины;

16) получение клиентом на банковскую карту денежных средств с одной (одного) или нескольких банковских карт или электронных кошельков, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины, одновременно или многократно в течение срока, не превышающего 30 дней;

17) перевод денежных средств через мобильное приложение с 5 и более банковских карт (электронных кошельков) на один иностранный электронный кошелек, одновременно или многократно в течение срока, не превышающего 30 дней;

18) поступление денежных средств на 5 и более банковских карт (электронных кошельков) с одного иностранного электронного кошелька, одновременно или многократно в течение срока, не превышающего 30 дней;

19) перевод денежных средств через мобильное приложение с одной (одного) банковской карты (электронного кошелька) на 5 и более иностранных банковских карт или электронных кошельков, одновременно или многократно в течение срока, не превышающего 30 дней;

20) поступление денежных средств с 5 и более иностранных банковских карт или электронных кошельков на 1 банковскую карту (электронный кошелек) одновременно или многократно в течение срока, не превышающего 30 дней.

7.3 Правление Банка может внедрять индикаторы раннего выявления сомнительных и подозрительных операций на основании методических рекомендаций, разрабатываемых Центральным банком Республики Узбекистан по согласованию с СУГО.

7.4 Работники должны уделять повышенное внимание всем сложным, необычно крупным операциям, а также всем необычным схемам совершения операций, не имеющим явной экономической или законной цели.

VIII. Порядок выявления и безотлагательного приостановления операций лиц, включенных в Перечень, замораживания денежных средств или иного имущества указанных лиц, а также направления их обращений по предоставлению доступа к замороженным денежным средствам или иному имуществу

8.1 Служба внутреннего контроля до начала рабочего дня, следующего за днем поступления в Банк Перечня, должна принять меры по:

1) внесению Перечня в автоматизированную банковскую систему (АБС) или иные программные обеспечения (при наличии), используемые для выявления лиц, включенных в Перечень, либо обновление Перечня, ранее внесенного в АБС;

2) направлению бумажной или электронной копии Перечня ответственным подразделениям либо непосредственно их работникам и (или) внесению электронной копии Перечня в общую базу (при наличии), доступную всем работникам в режиме просмотра.

8.2 Ответственные подразделения (Департамент информационных технологий, Департамент исполнительного аппарата (канцелярии и др.)) при необходимости должны содействовать Службе внутреннего контроля в осуществлении функций в соответствии с настоящими Правилами и внутренними документами.

8.3 В случае получения от Службы внутреннего контроля бумажной копии Перечня руководители ответственных подразделений Банка должны принять незамедлительные меры по доведению Перечня до работников до начала рабочего дня, следующего за днем поступления Перечня в Банк.

8.4 В случае отсутствия возможности использования программного обеспечения, позволяющего сверку данных участников операций с Перечнем в автоматическом режиме, Работники при проведении операций обязаны производить такую сверку в ручном режиме.

8.5 При проведении операций, в том числе через своих платежных агентов и (или) платежных субагентов, необходимо сверять идентификационные данные их участников с Перечнем.

В случае установления полного совпадения всех идентификационных данных клиента или одного из участников операции с лицом, включенным в Перечень, подобная операция подлежит безотлагательному приостановлению, а денежные средства или иное имущество, используемые в операции, подлежат замораживанию, за исключением операций по зачислению денежных средств, поступивших на счет физического или юридического лица.

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:

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

2) денежные средства или иное имущество, используемые для проведения операции, полностью или частично принадлежат лицу, включенному в Перечень;

3) юридическое лицо — участник операции, находится в собственности или под контролем лица, включенного в Перечень.

Требования настоящего пункта распространяются также на операции,

осуществляемые без открытия клиентам счетов (в том числе, выдачи наличной национальной или иностранной валюты из банковских карт, эмитированных другими банками, размены, замены, обмена или конверсии национальной или иностранной валюты, приобретение у физических лиц наличной иностранной валюты, аренда депозитных ячеек и т.д.).

8.6 Если во время установления отношений или при проведении операции, будет установлено полное совпадение всех идентификационных данных клиента или одного из участников операции с лицом, включенным в Перечень, работники должны:

1) без предварительного уведомления клиента приостановить проведение операции (за исключением операций по зачислению денежных средств, поступивших на счет юридического или физического лица) до момента тщательной перепроверки сотрудниками Службы внутреннего контроля факта совпадения;

2) незамедлительно и без уведомления клиента связаться (по телефону или другим, доступным каналам связи) с сотрудниками Службы внутреннего контроля для тщательной перепроверки информации;

3) в случае подтверждения сотрудником Службы внутреннего контроля факта полного совпадения:

а) не возобновлять проведение операции до получения письменного распоряжения Банка о приостановлении операции и замораживании денежных средств или иного имущества;

б) уведомить непосредственного руководителя о факте совпадения;

в) направить письменное сообщение в Службу внутреннего контроля, оформленное по форме, указанной в Приложении 5 к настоящим Правилам в день выявления совпадения;

г) следовать указаниям Службы внутреннего контроля.

8.7 В случае получения сообщения от работника о выявлении совпадения в порядке, установленном в пункте 8.5 настоящих Правил, Служба внутреннего контроля должна безотлагательно перепроверить сообщение, в том числе путем подробной идентификации личности клиента, бенефициарного собственника клиента либо одного из участников операции, по мере возможности.

8.8 В случае подтверждения факта полного совпадения всех идентификационных данных клиента или одного из участников операции с лицом, включенным в Перечень, Служба внутреннего контроля должна принять меры по:

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

2) изданию распоряжения Банка о приостановлении операции и замораживании денежных средств или иного имущества, используемых в операции, с незамедлительным направлением ответственному подразделению Банка не позднее дня выявления (подтверждения) совпадения;

3) подготовке и направлению в СУГО сообщения по данной операции с

указанием суммы замороженных денежных средств или имущества;

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

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

6) занесению информации об операции в специальный журнал.

8.9 Распоряжение Банка, оформляемое в соответствии с требованиями настоящей Главы, подписывается Председателем Правления (а при его отсутствии первым заместителем или заместителем Председателя Банка в случае отсутствия первого), главным бухгалтером, руководителями Службы внутреннего контроля и юридической службы.

В случаях, когда операция должна быть проведена с использованием транзитного счета Банка (или без открытия счета клиенту), замораживание денежных средств, используемых в данной операции, осуществляется путем их зачисления на отдельный балансовый счет обязательств, что должно быть указано в распоряжении Банка.

8.10 До момента издания и исполнения распоряжения Банка о приостановлении операции и (или) замораживании денежных средств или иного имущества работникам запрещается любыми методами информировать клиента или других участников о фактических причинах временного приостановлении осуществления (проведения) их операций. При обращении клиента по поводу задержки исполнения его поручений работник должен следовать устным указаниям сотрудника Службы внутреннего контроля.

Работники могут проинформировать клиента о приостановлении его операции и (или) замораживании денежных средств или иного имущества, только после полного завершения выполнения мер по приостановлению операции и замораживанию денежных средств или иного имущества, используемого в его операции в соответствии с распоряжением Банка.

8.11 В случае приостановления операции списание денежных средств со счетов, на основании распоряжения (поручения, заявления и т.д.) клиента не производится, а распоряжения (платежные документы) клиента передаются работниками в Службу внутреннего контроля.

Распоряжение клиента должно регистрироваться Службой внутреннего контроля в отдельном журнале по регистрации распоряжений клиентов (Приложение 6 к настоящим Правилам), операции которых приостановлены, а также помещаться в специальную папку до момента возобновления операции.

Замораживание осуществляется работниками в отношении денежных средств или иного имущества, которое находится в непосредственном владении (или распоряжении) Банка.

В отдельном журнале для регистрации распоряжений клиентов, операции которых приостановлены, фиксируется информация, позволяющая идентифицировать

операцию, которая была приостановлена, а также участников данной операции.

8.12 В соответствии с требованиями Положения 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 (далее — Положение о порядке приостановления/замораживания/предоставления доступа) возобновление приостановленных операций осуществляется в случаях:

- 1) исключения лица из Перечня;
- 2) приостановления операции лица, имеющего схожие идентификационные данные с лицом, включенным в Перечень (ложное срабатывание).

8.13 Возобновление операций и размораживание денежных средств или иного имущества осуществляется в соответствии с распоряжением Банка:

- 1) в течение трех рабочих дней со дня получения обновленного Перечня, в случае исключения лица из Перечня;
- 2) не позднее следующего рабочего дня со дня получения уведомления СУГО о факте приостановления Банком операции и замораживания денежных средств или иного имущества лица, имеющего схожие идентификационные данные с лицом, включенным в Перечень (ложное срабатывание).

Распоряжение Банка о возобновлении операций и размораживании денежных средств или иного имущества готовится Службой внутреннего контроля в порядке, установленном в пункте 8.12 настоящих Правил.

8.14 В соответствии с Положением о порядке приостановления/замораживания/предоставления доступа лицо, включенное в Перечень, в целях обеспечения базовых жизненных нужд, вправе обратиться в Банк для получения доступа к замороженным Банком денежным средствам и имуществу.

Обращение лица, включенного в Перечень, для получения доступа к замороженным Банком денежным средствам и имуществу принимается в письменном виде, адресованному Председателю Правления или одному из его заместителей.

К обращению прилагаются сведения о цели (которые должны соответствовать Положению о порядке приостановления/замораживания/предоставления доступа), сумме и обосновании платежа, виде замороженного имущества, реквизиты и идентификационные данные получателя денежных средств или иного имущества, банке получателя денежных средств.

8.15 Письменное обращение принимается управлением канцелярии, и вне зависимости от наличия резолюции руководства направляется в Службу внутреннего контроля в день его поступления для принятия оперативных мер.

Служба внутреннего контроля не позднее одного рабочего дня после получения Банком обращения направляет его в СУГО.

8.16 После получения информации СУГО о решении, принятом в целях предоставления лицу, включенному в Перечень, доступа к замороженному имуществу,

Служба внутреннего контроля в день получения такой информации должна принять меры по оформлению и направлению соответствующему подразделению Банка распоряжения, подготовленного в порядке, установленном в пункте 8.12 настоящих Правил.

Распоряжение Банка о предоставлении доступа к замороженному имуществу и денежным средствам должно соответствовать принятому компетентным государственным органом решению.

8.17 Операция, к которой предоставлен доступ, включая попытку ее проведения, признается подозрительной и подлежит сообщению в СУГО в порядке, установленном законодательством Республики Узбекистан и настоящими Правилами. В частности, работники, осуществляющие операции в рамках предоставленного клиенту доступа к замороженным средствам или иному имуществу должны направить письменное сообщение о подозрительной операции в Службу внутреннего контроля по форме, согласно Приложению 5 к настоящим Правилам в день осуществления операции.

IX. Порядок осуществления мер по изучению, анализу, выявлению, оценке, мониторингу, управлению, снижению и документированию риска

9.1 Изучение, анализ, выявление, оценка, мониторинг, управление, снижение и документальное фиксирование уровня риска в Банке осуществляется на основании требований законодательства Республики Узбекистан и настоящих Правил.

Департамент внутреннего контроля и комплаенс до завершения каждого финансового года, совместно с подразделениями Банка, ответственными за организацию и контроль банковских операций должна 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.

9.2 Департаментом внутреннего контроля и комплаенс совместно с подразделением Риск менеджмента, в зависимости от типов и уровня выявленных рисков должна быть разработана и реализована программа мер, для снижения рисков. Программа утверждается Председателем Правления.

В целях эффективного распределения ресурсов программа должна включать в себя необходимость применения усиленных мер в случае выявления высокого и упрощенных мер в случае выявления низкого уровня рисков.

9.3 Уровень риска выявляется и оценивается Службой внутреннего контроля на основании:

1) результатов надлежащей проверки клиента, в том числе представленной клиентом информации с учетом видов деятельности и операций, совершаемых клиентом;

2) письменных сообщений работников о выявлении сомнительной или подозрительной операции;

3) критериев, установленных законодательством Республики Узбекистан и настоящими Правилами;

4) факторов риска (по клиентам, странам и географическим регионам).

9.4 В результате оценки клиенту или операции, совершаемой клиентом, система присваивает уровень риска (высокий или низкий), который отражается в анкете клиента. Также, в анкете Службы внутреннего контроля должно быть зафиксировано основание для отнесения клиента или его операции к высокому уровню риска.

9.5 Результаты оценки риска должны быть представлены в Центральный банк Республики Узбекистан Департаментом внутреннего контроля и комплаенс.

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

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

2) лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в области ПОД/ФТ/ФРОМУ;

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

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

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

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

7) организации, бенефициарным собственником которых является лицо, указанное в подпунктах 1) и 2) настоящего пункта;

8) клиенты, осуществляющие подозрительные или сомнительные операции на систематической основе (например, два и более раза подряд в течение периода, не превышающего 3 месяцев);

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

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

11) иностранная структура без образования юридического лица;

12) лица, на аккаунты которых прикреплены 20 и более банковских карт;

13) другие лица, не подпадающие под критерии и не имеющие признаки, предусмотренных в данном пункте, но характер деятельности, которых предполагает отнесение их к клиентам с высоким уровнем риска

9.7 К категории высокого уровня риска Служба внутреннего контроля обязана отнести операции, отвечающие следующим критериям и в отношении которых работники должны проявлять повышенное внимание:

- 1) операции, участниками которых являются лица, указанные в подпунктах 1), 2), 8) и 11) пункта 9.6 настоящих Правил;
- 2) операции, осуществляемые через счета, открытые в оффшорных зонах;
- 3) операции с драгоценными металлами, драгоценными камнями, а также ювелирными изделиями, содержащими драгоценные металлы и драгоценные камни, за исключением таких операций, проводимых самим Банком;
- 4) 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;
- 5) другие операции, не отвечающие критериям и не имеющие признаков, предусмотренных в данном пункте, но характер которых предполагает отнесение их к операциям с высоким уровнем риска.

9.8 При отнесении клиента или операции, осуществляемой клиентом, к категории высокого уровня риска работники и (или) Служба внутреннего контроля (в зависимости) должны применять усиленные меры надлежащей проверки в отношении такого клиента или его операции.

9.9 По мере изменения характера проводимых клиентом операций Служба внутреннего контроля при необходимости должна пересматривать уровень риска работы с ним.

9.10 Учет клиентов, отнесенных к высокому уровню риска, осуществляется непосредственно Службой внутреннего контроля.

Служба внутреннего контроля ведет электронный учет клиентов и операций с высоким уровнем риска в целях осуществления мониторинга рисков и составления отчетности, представляемой в Центральный банк Республики Узбекистан и руководству Банка.

9.11 В целях снижения рисков Правление, ответственные подразделения, их работники и Департамент внутреннего контроля и комплаенс, в рамках своих полномочий, должны принимать меры по своевременному и качественному исполнению соответствующих требований законодательства Республики Узбекистан и настоящих Правил.

9.12 Правление, ответственные подразделения Банка и Департамент внутреннего контроля и комплаенс должны принимать меры по недопущению злоупотребления технологическими достижениями в целях ОД/ФТ. В этих целях необходимо определять и оценивать уровни риска, которые могут возникнуть в связи с:

- 1) разработкой новых видов услуг и новой деловой практики;
- 2) использованием новых или развивающихся технологий как для новых, так и для уже существующих видов услуг.

9.13 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 ответственным подразделением Банка, непосредственно внедряющим новые виды услуг (новую технологию), совместно с Департаментом внутреннего контроля и комплаенс.

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

Информация о результатах осуществленных мер должна предоставляться Правлению Банка, ответственными подразделениями Банка и Департаментом внутреннего контроля и комплаенс.

9.14 В целях снижения риска ответственные подразделения Банка, предоставляющие дистанционные услуги:

1) 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;

2) должны отказать в предоставлении услуги в случае выявления подозрительных операций, осуществленных клиентом с использованием таких услуг;

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

9.15 Комплексный анализ должен проводиться банком при подключении клиента к системам дистанционного обслуживания (мобильное приложение, вебсайты, телеграмм боты) или обращении клиента с намерением установить деловые отношения либо осуществить операцию с денежными средствами или иным имуществом. В отдельных случаях, прямо предусмотренных законодательством, комплексный анализ может проводиться после осуществления операции.

1) Срок проведения комплексного анализа не должен превышать сроков направления сообщения о подозрительной операции в СУГО, установленный законодательством.

2) Отдельные элементы комплексного анализа необходимо автоматизировать с целью сокращения трудозатрат на его проведение.

Комплексный анализ состоит из следующих элементов:

а) анализ имеющихся и доступных данных о клиенте;

б) изучение профиля рисков клиента и сообщений о подозрительных операциях, ранее отправленных в СУГО в отношении клиента;

в) изучение цели и характера деловых отношений и операции, включая анализ ранее осуществленных операций;

г) изучение деталей операции.

В официальной оферте по предоставлению услуг должно отражаться полномочие платежных организаций по получению от клиента информации в части идентификации

и надлежащей проверки клиента.

3) В ходе анализа имеющихся и доступных данных о клиенте физическом лице целесообразно обращать внимание на следующие моменты:

а) данные клиента, которые включают проведение идентификации и верификации участников финансовой операции в соответствии с законодательством Республики Узбекистан и фиксирование информации в электронной базе данных анкет клиентов с возможностью оперативного доступа к ней уполномоченных работников;

В частности, при идентификации клиентов, применяется принцип «Знай своего клиента» с детальным изучением характера и цели запланированных операций, принадлежности к категории ПДЛ, получением дополнительной информации об источниках доходов/средств, вида занятости клиентов и т.д. Подобные меры в конечном итоге способствуют более четкому представлению будущих операций с клиентами, определению возможных рисков для дальнейшего управления этими рисками;

б) выявление из числа клиентов иностранных публичных должностных лиц, должностных лиц публичных международных организаций, членов их семей и приближенных к ним лиц, а также организаций;

в) место постоянного проживания;

г) объем и количество транзакций проводимой операции;

д) использование клиентом программного обеспечения дистанционного обслуживания;

е) наличие прикрепленных карт на мобильное приложение, в том числе собственные и на чужие карты;

ё) наличие банковских карт и электронных кошельков;

ж) получение идентификационных данных клиента от третьих лиц или из ведомственных баз данных (Агентство государственных услуг, паспортный стол МВД, консульское управление МИД);

з) сбор дополнительной информации о клиенте, контрагенте, связанных с ними лицах, и деталях операции может осуществляться из коммерческих банков, платежных организаций, открытых источников Интернет, средств массовой информации;

4) При анализе характера запланированных операций целесообразно сопоставлять операции клиента с результатом анализа использования платежных услуг за прошедший период:

а) сопоставить цели и характер операции с результатом изучения ранее осуществленных операций для установления ее соответствия обычной деятельности клиента;

б) проанализировать сведения о контрагенте по операции, в том числе в целях выявления других клиентов, осуществляющих отправку денежных средств в адрес данного контрагента;

в) проанализировать ранее совершенные сходные операции (в том числе операции других клиентов) на предмет выявления отправленных по ним сообщений о

подозрительных операциях;

г) изучать односторонние и двухсторонние операции, проводимые между клиентом и его партнерами (контрагент) на предмет сомнительности. Цели проводимых операций, сумма и периодичность их осуществления.

Банк должен усилить мониторинг при совершении операции через мобильное приложение, где владелец аккаунта и владелец прикрепленной карты разные лица, а также по мере возможности установить аффилированность или другую связь этих лиц.

При проведении анализа рекомендуется изучить сведения о полномочиях владельца аккаунта, наличии полномочий или прав (доверенность или другие документы) на осуществление операций от имени владельца карты.

Особого внимания заслуживает изучение истории клиента на предмет выявления ранее отправленных сообщений о совершенных ими подозрительных операциях в СУГО.

5) При проведении анализа данных о клиенте - физическом лице, являющемся публичным должностным лицом, в дополнение к мерам, указанным в предыдущем пункте, целесообразно:

а) изучить и подтвердить через доступные источники (открытые данные Интернет, средств массовой информации, ведомственные или зарубежные коммерческие базы данных) сведения о статусе публичного должностного лица;

б) потребовать от клиента и изучить сведения об источниках денежных средств или иного имущества, используемых при проведении операции;

в) получить разрешение руководителя организации на подписание договора и/или продолжение отношений с клиентом, являющимся публичным должностным лицом.

б) Первичный сбор информации для комплексного анализа осуществляется соответствующими сотрудниками банка и операторами электронных денег. Полный комплексный анализ операций проводится сотрудниками комплаенс контроля.

Сотрудники комплаенс контроля должны собирать, анализировать и фиксировать результаты комплексного анализа. При наличии достаточных оснований, операция признается подозрительной.

При направлении сообщения о подозрительной операции в СУГО необходимо указывать в качестве дополнительной информации результаты комплексного анализа, послужившие основанием для признания операции подозрительной, с приложением соответствующих документов и сведений.

Х. Выявление сомнительных и подозрительных операций, а также подготовка и направление сообщений о подозрительных операциях в специально уполномоченный государственный орган

10.1 Информация, полученная в ходе идентификации, а также присвоенный уровень риска клиенту являются основой для мониторинга операций, осуществляемых

(осуществленных) клиентами, проводимого для того, чтобы убедиться в соответствии таких операций основным направлениям деятельности клиента, и изучения при необходимости источников средств.

10.2 Идентификация клиентов и текущая проверка их операций проводится работниками подразделений Банка, непосредственно обслуживающими клиентов (ответственными исполнителями, кассирами и т. п.) в соответствии с должностными обязанностями, которые при выявлении операций, имеющих признаки подозрительных и (или) сомнительных операций, обязаны незамедлительно (в день выявления) в письменном виде сообщить о таких операциях своему непосредственному руководителю и сотрудникам Службы внутреннего контроля.

10.3 Письменные сообщения о сомнительных и подозрительных операциях оформляются по формам, согласно Приложениям 4 и 5 к настоящим Правилам.

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

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

10.6 После получения письменного сообщения работника о выявлении сомнительных и подозрительных операций сотрудники Службы внутреннего контроля должны:

- 1) внести соответствующую информацию в специальный журнал и анкету клиента;
- 2) изучить сведения о клиенте и операции;
- 3) при наличии достаточных оснований направить (внести) руководителю Службы внутреннего контроля предложение о классификации операции как сомнительной или подозрительной.

10.7 При наличии обоснованных подозрений руководитель Службы внутреннего контроля принимает письменное решение о признании операции клиента подозрительной и в случае необходимости, информирует Председателя Правления Банка (при его отсутствии, уполномоченного заместителя Председателя Банка).

10.8 Признание операций подозрительными осуществляется в каждом конкретном случае на основе комплексного анализа, проводимого с использованием критериев и признаков, установленных законодательством Республики Узбекистан и настоящими Правилами.

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

- 1) предоставить сообщение о подозрительной операции в СУГО в случаях:
 - а) признания операции подозрительной (проведённой или попытке её

проведения);

б) признания операции высокорискованной, по результатам национальной оценки рисков, связанной с легализацией преступных доходов;

в) приостановления операции, связанной с лицами или организациями, включёнными в ПЕРЕЧЕНЬ;

г) приостановления операции в результате проверок;

д) отказа в - открытии счета, проведение транзакции, вступления в деловые отношения и прекращении существующих деловых отношений;

е) невозможности осуществления надлежащей проверки клиента.

2) получить дополнительную информацию о клиенте;

3) пересмотреть уровень риска клиента;

4) усилить мониторинг за операциями клиента;

10.10 Сообщение о подозрительной операции передается Службой внутреннего контроля в СУГО в соответствии с требованиями Положения о порядке предоставления информации, связанной с ПОД/ФТ. Сообщение должно сопровождаться информацией, на которой оно основано, а также подтверждающими документами.

10.11 Информация о каждом сообщении заносится в специальный журнал. Специальный журнал ведется в электронном виде.

При формировании таких таблиц не требуется переносить электронное сообщение на бумажный носитель. Сообщение, отправленное в СУГО, 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 сотрудником Службы внутреннего контроля на основании полномочий, письменно предоставленных ему Председателем Правления Банка.

10.12 При наличии любой информации, которая может подтвердить или снять подозрения с соответствующей операции работники обязаны незамедлительно представить её в Службу внутреннего контроля, которая должна сообщить о ней в СУГО.

XI. Порядок направления запросов специально уполномоченным государственным органом

11.1 СУГО вправе направить в банк запрос о предоставлении информации и должным образом заверенных копий документов в целях соблюдения законодательства и выполнения обязательств в области ПОД/ФТ. По запросу СУГО банк обязуется бесплатно предоставлять запрашиваемую информацию в соответствии с требованиями Положения о порядке предоставления информации, связанной с ПОД/ФТ. Электронные запросы подтверждаются электронной цифровой подписью, а бумажные запросы оформляются на официальном бланке СУГО, подписываются его руководителем или заместителем руководителя и отправляются по электронным каналам связи, лично или

специальной почтой. Банк направляет запрашиваемую информацию в СУГО в электронном виде в течение трех рабочих дней со дня получения запроса с подтверждением в электронном виде по каналам связи, лично или по специально предназначенной почте. С учетом объема, характера и содержания запрашиваемой информации СУГО может быть установлен иной срок их предоставления.

XII. Оформление, хранение, обеспечение конфиденциальности информации и документов

12.1 Документы, связанные с надлежащей проверкой клиентов, составленные полностью или в какой-либо их части на иностранном языке, должны быть истребованы работником, при необходимости, с переводом на государственный или русский язык.

12.2 В случае возникновения сомнений в достоверности представленных копий документов или другой необходимости работник вправе потребовать представления подлинников документов для ознакомления.

12.3 Информация о клиенте, полученная в процессе надлежащей проверки клиента, указывается в анкете клиента согласно Приложению 3 к настоящим Правилам. Служба внутреннего контроля вправе включить в анкету клиента другие данные.

12.4 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.

12.5 Анкета клиента хранится в электронной базе Банка не менее пяти лет со дня прекращения отношений с клиентом.

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

12.7 Информация об операциях должна быть оформлена таким образом, чтобы в случае необходимости было возможно восстановить детали операции.

12.8 Ответственные подразделения, их работники и Служба внутреннего контроля обязаны хранить информацию об операциях, а также идентификационные данные и материалы по надлежащей проверке клиентов, файлы счетов и деловую переписку, результаты любого проведенного анализа в течение сроков, установленных законодательством, но не менее пяти лет после осуществления операций или прекращения деловых отношений с клиентами.

Указанные сведения и документы должны храниться на бумажном и (или) электронном носителях в формате, обеспечивающем их своевременное представление уполномоченным государственным органам и Центральному банку.

12.9 В целях ограничения доступа к документам (переписка с Центральным банком и СУГО, в том числе электронные копии переданных в СУГО сообщений; электронные анкеты клиентов; журналы и др.), использованным в деятельности Службы

внутреннего контроля, такие документы и их опись должны храниться непосредственно Службой внутреннего контроля в специально обустроенных помещениях или в негорючем и опечатываемом сейфе в течение сроков, установленных законодательством Республики Узбекистан, но не менее пяти лет.

По истечении сроков хранения документы сдаются в установленном порядке в архив Банка.

12.10 Ответственные подразделения, их работники и Служба внутреннего контроля ограничивают доступ к информации, связанной с ПОД/ФТ/ФРОМУ, в том числе к документам, хранящимся в архивах Банка, обеспечивают ее нераспространение и не вправе информировать юридические и физические лица о предоставлении сообщений об их операциях в СУГО.

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

12.12 Сведения, полученные в результате надлежащей проверки клиента, должны обновляться исходя из значимости и рисков, и при наличии изменений в сведениях клиента, но не реже одного раза в год в случаях, когда Служба внутреннего контроля 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.

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

XIII. Квалификационные требования к подготовке и обучению кадров

13.1 Служба внутреннего контроля, подразделения Банка, непосредственно обслуживающие клиентов, юридическая служба, службы внутреннего аудита и безопасности обязаны проводить переподготовку своих работников с целью обеспечения их информированности о последних новинках, включая информацию по современной технике легализации доходов, полученных от преступной деятельности, финансирования терроризма и финансированию распространения оружия массового уничтожения, методах и тенденциях, и четкого разъяснения всех аспектов законодательства и обязательств по ПОД/ФТ/ФРОМУ.

13.2 Квалификационные требования к подготовке и обучению работников по вопросам по ПОД/ФТ/ФРОМУ устанавливаются внутренними нормативными документами Банка.

13.3 Служба внутреннего контроля совместно с соответствующими подразделениями Банка ежегодно разрабатывает Программу подготовки, переподготовки и обучения работников Банка по вопросам ПОД/ФТ/ФРОМУ. Данная

Программа должна предусматривать:

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

XIV. Ответственность сотрудников Службы внутреннего контроля и других подразделений

14.1 Сотрудники Служба внутреннего контроля и других подразделений несут ответственность за нарушение требований законодательства Республики Узбекистан и настоящих Правил.

14.2 Работники, которым стали известны факты нарушений законодательства Республики Узбекистан, в том числе в области ПОД/ФТ/ФРОМУ, допущенных работниками Банка при проведении операций, незамедлительно в письменном виде доводят эти факты до руководителя Службы внутреннего контроля.

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

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

XV. Заключительные положения

15.1 Правление Банка проводит постоянный мониторинг и оценку эффективности системы внутреннего контроля по ПОД/ФТ/ФРОМУ Банка с учетом изменяющихся внутренних и внешних обстоятельств, а также укрепляют ее по мере необходимости для обеспечения эффективной работы.

Мониторинг эффективности системы внутреннего контроля по ПОД/ФТ/ФРОМУ также может осуществляться службой внутреннего аудита Банка.

15.2 Недостатки системы внутреннего контроля по ПОД/ФТ/ФРОМУ, выявленные Службой внутреннего аудита или другими контрольными службами, своевременно доводятся до сведения Председателя Правления Банка. После получения такой информации Председатель Правления Банка должен обеспечить своевременное устранение выявленных недостатков.

15.3 Правила обязательны для исполнения платежными агентами и платежными субагентами, а также всеми подразделениями и офисами продаж. Банк должен вести актуализированный реестр своих платежных агентов и платежных субагентов, доступный компетентным органам в странах, в которых они, их агенты и субагенты действуют.

Приложение 1

к Правилам внутреннего контроля
в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ

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 идентификационной ID-карты или заменяющего их документа: серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ.
6. Персональный идентификационный номер физического лица (если имеется).
7. Номер домашнего телефона (если имеется).
8. Налоговое резиденство (в случае наличия подтверждающей информации).

Приложение 2

к Правилам внутреннего контроля
в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ

**ИНФОРМАЦИЯ
необходимая при идентификации юридических лиц и индивидуальных
предпринимателей**

1. Информация, необходимая при идентификации юридических лиц:

- 1) полное, а также сокращенное наименование, если оно указано в свидетельстве о государственной регистрации;
- 2) информация о государственной регистрации: дата, номер, наименование регистрирующего органа;
- 3) идентификационный номер налогоплательщика;
- 4) местонахождение (почтовый адрес) а также адрес зарегистрированного офиса и адрес головного офиса, если он отличается от первого;
- 5) другие данные, указанные в свидетельстве о государственной регистрации;
- 6) информация об имеющихся лицензиях на осуществление видов деятельности, подлежащих лицензированию: вид деятельности, номер и дата выдачи лицензии; кем выдана; срок действия;
- 7) данные об идентификации физических лиц, имеющих право подписи, или физического лица, действующего от имени юридического лица;
- 8) информация об учредителях (крупных акционерах, участниках) и об их долевых участиях в уставном фонде (капитале) юридического лица;
- 9) информация о величине зарегистрированного и оплаченного уставного фонда (капитала);
- 10) информация об органах управления юридического лица (структура и персональный состав органов управления юридического лица);
- 11) номера телефонов.

2. Информация, необходимая при идентификации индивидуальных предпринимателей:

- 1) информация, предусмотренная Приложением 1 к Правилам внутреннего контроля в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ;
- 2) информация о государственной регистрации: дата, номер, наименование регистрирующего органа;

- 3) место осуществления деятельности;
- 4) другие данные, указанные в свидетельстве о государственной регистрации;
- 5) информация об имеющихся свидетельствах и лицензиях на осуществление видов деятельности: вид деятельности, номер, дата выдачи; кем выдана; срок действия;
- 6) номера телефонов.

Приложение 3

к Правилам внутреннего контроля в АО "АРЕХ
BANK" по противодействию легализации доходов,
полученных от преступной деятельности,
финансированию терроризма и финансированию
распространения
оружия массового уничтожения

**ИНФОРМАЦИЯ,
указываемая в анкете клиента**

1. Информация, полученная в процессе идентификации клиента, указанная в Приложениях 1 и 2 к Правилам внутреннего контроля в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ.
 - a. Данные о бенефициарном собственнике клиента.
 - b. Отметка о том, является ли клиент публичным должностным лицом (членом его семьи или лицом, близким к публичному должностному лицу).
2. Информация об уровне риска, включая обоснование оценки риска.
3. Результаты дополнительных мероприятий, проведенных при идентификации клиента.
4. Дата начала отношений с клиентом — дата открытия первого банковского счета (вклада) в Банке.
5. Дата заполнения и внесения изменений в анкету клиента.
6. Фамилия, имя и отчество, должность работника, ответственного за работу с клиентом, в частности, работника, открывшего счет (главного бухгалтера или его заместителя) и утвердившего открытие счета.
7. Фамилия, имя и отчество, должность сотрудника, заполнившего анкету клиента.
8. Иные данные.

Приложение 4

к Правилам внутреннего контроля
в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ

**Департаменту по ПОД/ФТ/ФРОМУ и
санкционному комплаенсу
АО "АРЕХ BANK"****Сообщение о сомнительной операции**

В результате текущей проверки операции клиента _____
_____, (ИНН _____), проведенной _____ согласно
(наименование клиента)
прилагаемому платежному документу от _____ 20__ года, выявлена
сомнительная операция с признаком (критерием), указанным в подпункте ____ пункта
7.1 Правил внутреннего контроля АО "АРЕХ BANK" по противодействию легализации
доходов, полученных от преступной деятельности финансированию терроризма и
финансированию распространения оружия массового уничтожения.

Сумма операции:

Копия платежного документа прилагается.

Настоящим подтверждаю, что сведения, по данному сообщению, разглашению не
подлежат _____
(ФИО и подпись работника, предоставившего сообщение)

Дата сообщения _____

Отметка СВК _____
(дата получения сообщения)

(ФИО и подпись работника СВК)

Приложение 5

к Правилам внутреннего контроля
в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ

**Департаменту по ПОД/ФТ/ФРОМУ и
санкционному комплаенсу
АО "АРЕХ BANK"**

Сообщение о подозрительной операции

В результате текущей проверки операции клиента _____
_____, (ИНН _____), проведенной _____ согласно
(наименование клиента)

прилагаемому платежному документу от _____ 20__ года, выявлена
подозрительная операция с признаком (критерием), указанным в подпункте ____ пункта
7.2 Правил внутреннего контроля АО "АРЕХ BANK" по противодействию легализации
доходов, полученных от преступной деятельности финансированию терроризма и
финансированию распространения оружия массового уничтожения.

Сумма операции:

Копия платежного документа прилагается.

Настоящим подтверждаю, что сведения, по данному сообщению, разглашению не
подлежат _____
(ФИО и подпись работника, предоставившего сообщение)

Дата сообщения _____

Отметка СВК _____
(дата получения сообщения)

(ФИО и подпись работника СВК)

Приложение 6

к Правилам внутреннего контроля
в АО "АРЕХ BANK" по ПОД/ФТ/ФРОМУ

1. Вид обложки журнала:

АО "АРЕХ BANK"

Ж У Р Н А Л

**регистрации распоряжений клиентов,
операции которых приостановлены**

2. Форма таблицы в рабочей части журнала:

1) нечетные страницы:

№ п/ п	Дата приостанов ления операции	Наименов ание (или ФИО) клиента	Уникальн ый код клиента	Вид (содержание) приостановл енной операции	Дата документа (распоряж ения) клиента	Вид документа (распоряже ния) клиента
1	2	3	4	5	6	7

2) четные страницы:

Сумма опера ции	Сведения о контраген те клиента (наимено вание юр. лица или ФИО физ. лица)	Основан ие для приостан овления операци и	Дата проведен ия (возобнов ления) операции	Дата и номер предписан ия Департам ента о приостано влении операции	Дата проведен ия (возобнов ления) операции	Сотрудник, зарегистрир овавший приостановл енную операцию, и его подпись
8	9	10	11	12	13	14

