



ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в области противодействия легализации (отмыванию) преступных доходов и финансированию террористической деятельности (далее – «**Политика**»), является документом, раскрывающим основные правила и политики ОАО «БитРуби» (далее – «**Оператор**»), применяемые в области противодействия легализации (отмыванию) преступных доходов и финансированию террористической деятельности, и соблюдения требований законодательства в этой сфере при осуществлении деятельности оператора торгов виртуальных активов (криптовиржи) посредством Сервиса.

1.2. Национальное законодательство Кыргызской Республики требует от ОАО «БитРуби» осуществления мер по противодействию финансированию террористической деятельности и легализации (отмыванию) преступных доходов при осуществлении деятельности оператора торгов виртуальных активов (криптовиржи).

1.3. В целях реализации указанных мер Оператор осуществляет надлежащую проверку Пользователей Сервиса перед началом установления отношений с Пользователем и в иных случаях, предусмотренных законодательством и внутренними документами Оператора.

1.4. Мерами надлежащей проверки Пользователей являются:

1.4.1. идентификация и верификация Пользователя – физического и юридического лица, его бенефициарного владельца и представителя;

1.4.2. заполнение электронной анкеты Пользователем – физическим и юридическим лицом, его бенефициарным владельцем и представителем сведениями, полученными в результате идентификации и верификации Пользователя;

1.4.3. хранение и обновление информации, указанной в анкетах;

1.4.4. проведение на протяжении всего периода деловых отношений с Пользователем анализа соответствия операций (сделок) Пользователя с имеющейся информацией о его деятельности, финансовом положении и об источнике средств, а также о характере рисков ФТД/ЛПД.

1.5. Настоящая политика помимо прочего определяет порядок осуществления верификации Пользователя, уровни верификации и объем прав по использованию Сервиса, предоставляемый Пользователям в зависимости от их уровня верификации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Бенефициарный владелец** – физическое лицо (физические лица), которое в конечном итоге (через цепочку владения и контроля) прямо или косвенно (через третьих лиц) владеет правом собственности или контролирует Пользователя либо физическое лицо, от имени или в интересах которого совершается операция (сделка).

2.2. **Оператор** – Юридическое лицо, осуществляющее управление Сервисом, а также выполняющее функции по идентификации, верификации и мониторингу Операций Пользователей, а также реализующий иные полномочия, предусмотренные настоящей Политикой.

2.3. **Пользователь** – Физическое или юридическое лицо, прошедшее процедуру регистрации в Сервисе и осуществляющее Операции с использованием функциональных возможностей Сервиса.

2.4. **Верификация** – процедура проверки идентификационных данных Пользователя и (или) бенефициарного владельца.

2.5. **Высокорискованные страны** – государства и территории (образования), которые не применяют или применяют в недостаточной степени международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, а также офшорные зоны.

2.6. **Деловые отношения** – отношения между Пользователем и Оператора, возникшие на основе договоренности (устной или письменной) о предоставлении услуг по осуществлению операции (сделки).

2.7. **Замораживание операции (сделки) и (или) средств** – запрещение проведения операции (сделки) со средствами или передачи, преобразования, отчуждения и перемещения любых Средств.

- 2.8. **Идентификация** - процедура установления идентификационных данных о Пользователе и (или) бенефициарном владельце.
- 2.9. **Комплаенс-офицер** - уполномоченный сотрудник, ответственный за осуществление программ внутреннего контроля по ПФТД/ЛПД.
- 2.10. **Легализация (отмывание) преступных доходов** – уголовно наказуемое общественно опасное деяние, предусмотренное статьей 222 Уголовного кодекса Кыргызской Республики; придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, приобретёнными заведомо незаконным путём.
- 2.11. **Операции (сделки)** - любые операции (сделки) со средствами, совершаемые для установления, изменения или прекращения гражданских прав и обязанностей со Средствами.
- 2.12. **Пользовательское соглашение** – юридический документ, размещенный в Сервисе и регламентирующий отношения Оператора с Пользователем по поводу использования Сервиса Пользователем.
- 2.13. **Преступный доход** - доход (средства), полученный или извлеченный прямо или косвенно в результате совершения преступления на территории Кыргызской Республики или иностранного государства.
- 2.14. **Подозрительная операция**- Операция, в отношении которой у Оператора имеются основания полагать, что она может быть связана с легализацией (отмыванием) преступных доходов, финансированием террористической или экстремистской деятельности, либо иными противоправными действиями.
- 2.15. **Публичные должностные лица (далее - ПДЛ)** - одно из следующих физических лиц:
- 2.15.1. **Иностранное публичное должностное лицо** - лицо, выполняющее или выполнявшее значительные государственные или политические функции (публичные функции) в иностранном государстве (главы государств или правительств, высшие должностные лица в правительстве и иных государственных органах, судах, вооруженных силах, на государственных предприятиях, а также видные политические деятели, в том числе видные деятели политических партий);
- 2.15.2. **Национальное публичное должностное лицо** - лицо, занимающее или занимавшее политическую и специальную государственную должность или политическую муниципальную должность в Кыргызской Республике, предусмотренную Реестром государственных и муниципальных должностей Кыргызской Республики, утверждаемым Президентом Кыргызской Республики, а также высшее руководство государственных корпораций, видные политические деятели, в том числе видные деятели политических партий;
- 2.15.3. **Публичное должностное лицо международной организации** - высшее должностное лицо международной организации, которому доверены или были доверены важные функции международной организацией (руководители, заместители руководителей и члены правления международной организации или лица, занимающие эквивалентные должности в международной организации).
- 2.16. **Санкционный перечень** - перечень физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об их участии в террористической или экстремистской деятельности и распространении оружия массового уничтожения (Сводный санкционный перечень Кыргызской Республики; Сводный санкционный перечень Совета Безопасности ООН; Санкционные списки OFAC и ЕС).
- 2.17. **Финансирование распространения оружия массового уничтожения** - предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что средства предназначены или будут использованы полностью или частично для финансирования распространения ядерного, химического и биологического оружия и (или) средств его доставки.
- 2.18. **Финансирование террористической или экстремистской деятельности** - уголовно наказуемые общественно опасные деяния, предусмотренные статьями 253 и 331в Уголовном кодексе Кыргызской Республики; предоставление или сбор денег и (или) иного имущества либо оказание финансовых услуг террористам и/или террористическим (экстремистским) организациям для осуществления террористической (экстремистской) деятельности.
- 2.19. **ПФТД/ЛПД**- Сокращение, обозначающее «Противодействие финансированию террористической деятельности и легализации (отмыванию) преступных доходов».

Иные термины, написанные с заглавной буквы и применяющиеся в настоящем документе должны иметь значение, установленное Пользовательским соглашением.

3. ВЕРИФИКАЦИЯ

3.1. В целях проведения первичной верификации Пользователя Пользователь обязан заполнить анкету, доступную в Сервисе и направить ее Оператору с помощью технических средств, доступных в Сервисе. При заполнении анкеты Пользователь обязуется предоставлять точную, достоверную и корректную информацию. В случае выявления Оператором недостоверности информации, Оператор вправе запросить разъяснения у Пользователя по поводу недостоверной информации или прекратить дальнейшие отношения с таким Пользователем по своему усмотрению и без объяснения причин.

3.2. Для верификации личности Пользователя-физического лица, а также бенефициарного владельца и представителя Пользователя-юридического лица, Оператор использует один из следующих документов, удостоверяющих личность:

3.2.1. в отношении граждан КР:

3.2.1.1. паспорт гражданина Кыргызской Республики образца 2004 года (ID-карта);

3.2.1.2. идентификационная карта - паспорт гражданина Кыргызской Республики образца 2017, 2024 годах (ID-карта);

3.2.1.3. свидетельство органов ЗАГС о рождении гражданина - для гражданина Кыргызской Республики, не достигшего 18 лет;

3.2.1.4. военный билет;

3.2.1.5. водительское удостоверение.

3.2.2. в отношении иностранных граждан:

3.2.2.1. паспорт иностранного гражданина;

3.2.2.2. вид на жительство в Кыргызской Республике.

3.2.3. в отношении беженцев:

3.2.3.1. свидетельство о регистрации ходатайства о признании лица беженцем;

3.2.3.2. удостоверение беженца.

3.3. Для верификации Пользователя-индивидуального предпринимателя помимо документов, указанных в п. 3.2. Оператор использует документ установленной формы, выданный уполномоченным органом и подтверждающий факт прохождения государственной регистрации (перерегистрации) (свидетельства) в качестве индивидуального предпринимателя, или копию документа, подтверждающего факт занятия предпринимательской деятельностью без государственной регистрации (патента) в случаях, предусмотренных законодательством Кыргызской Республики.

3.4. Для верификации Пользователя-юридического лица Оператор использует следующие документы:

3.4.1. решение учредителя (учредителей) о создании юридического лица;

3.4.2. устав и учредительный договор (если предусмотрено законодательством страны регистрации юридического лица);

3.4.3. свидетельство о государственной регистрации (перерегистрации) юридического лица;

3.4.4. изменения (дополнения) в учредительные документы (решение, устав, учредительный договор) - при перерегистрации юридического лица;

3.4.5. документ, подтверждающий постановку на учет в налоговом органе;

3.4.6. документы, подтверждающие полномочия лиц, имеющих право первой и второй подписи в карточке с образцами подписей и оттиском печати (решения органов управления, приказы, доверенности);

3.4.7. лицензии на право осуществления предпринимательской деятельности (при наличии).

3.5. При верификации Пользователя Оператор использует подлинники документов, действительные на дату их предъявления, или их копии, заверенные нотариусом, либо отсканированные документы от Пользователя, полученные по защищенным и проверенным электронным каналам связи (мобильное приложение/интернет-сервис/электронная почта), в том числе с применением электронной подписи Пользователя. Если для верификации Пользователя достаточно предоставление лишь части документа, Пользователем может быть представлена выписка из него, заверенная нотариусом.

3.6. В случае, если документы составлены полностью или частично на иностранном языке, Оператор может потребовать от Пользователя перевод документа на государственный или официальный язык, заверенный переводческим учреждением.

3.7. Документы, исходящие от государственных органов иностранных государств, подтверждающие статус юридических лиц-нерезидентов, принимаются Оператором только в случае их легализации (или при наличии на них апостиля, проставленного в предусмотренном международными договорами порядке).

3.8. Оператор при осуществлении верификации Пользователя вправе прибегать к услугам независимых третьих лиц, в том числе, но не ограничиваясь к услугам SUMSUB TECH LTD и аффилированных с ним лиц. Пользователь, инициируя верификацию, даёт согласие Оператору на передачу персональных данных Пользователя, требуемых для прохождения Пользователем верификации, таким третьим лицам, в том числе компании SUMSUB TECH LTD и аффилированным с ним лицам.

3.9. Оператор самостоятельно может присуждать уровень риска Пользователя в соответствии с внутренними политиками Оператора. При этом Оператор вправе присудить один из двух уровней риска Пользователю: высокий уровень риска и низкий уровень риска.

3.10. Оператор вправе запрашивать иные документы, не указанные в настоящем разделе 3 у Пользователей, которым присужден высокий уровень риска, в целях проведения надлежащей проверки таких Пользователей и совершаемых ими посредством Сервиса Сделок.

4. УРОВНИ ВЕРИФИКАЦИИ

4.1. Пользователи могут получить доступ к операциям на Сервисе XRuby только после прохождения полной процедуры верификации. Верификация включает:

- 4.1.1. подтверждение контактной информации (e-mail, телефон);
- 4.1.2. заполнение анкет юр. лица и бенефициаров для пользователей – юридических лиц;
- 4.1.3. предоставление данных
- 4.1.4. предоставление учредительных документов и удостоверений личности;
- 4.1.5. отправку всех материалов на адрес: aml@xruby.kg.

4.2. Проверка данных по Пользователям – юридическим лицам, их бенефициарным владельцам и представителям осуществляется комплаенс-офицером самостоятельно. До завершения верификации операции на платформе недоступны.

Для Пользователей – юридических лиц

Уровень верификации	Условия прохождения	Требования к документам	Способ передачи	Макс. лимит депозита (в день)	Макс. лимит вывода (в день)
Уровень 0 (верификация не пройдена)	Регистрация в Сервисе XRuby, подтверждение e-mail;	–	Подтверждение адреса e-mail посредством ввода временного одноразового OTP-кода, направленного на почту.	Пользователь вправе ознакомиться с функционалом Сервиса. Возможность осуществления открытия Кошелька или совершения Сделок с использованием Сервиса недоступна.	Пользователь вправе ознакомиться с функционалом Сервиса. Возможность осуществления открытия Кошелька или совершения Сделок с использованием Сервиса недоступна.
Уровень 1	Верификация номера мобильного телефона; Заполнение анкет; Предоставление полного пакета KYC-документов: 1. Анкета юридического лица; 2. Анкета бенефициарного владельца; 3. Анкета представителя; 4. Учредительные документы согласно п. 3.4.; 5. Паспорт бенефициарного владельца;	Предоставление оригиналов анкет; нотариально заверенных скан-компаний, хорошо читаемых, учредительных документов; документы, а также документы, удостоверяющие личность, составленные на иностранном языке, должны быть переведены на русский язык и нотариально заверены.	Подтверждение номера телефона посредством ввода временного одноразового OTP-кода, направленного указанный в Сервисе XRuby телефон. Отправка пакета документов на почту aml@xruby.kg Предоставление оригиналов заполненных анкет.	Кыргызский сом - 45 000 000 KGS/ сут. 500 000 USDT (Доллар США)/ сут. <i>(и эквивалент в других валютах)</i>	Кыргызский сом - 15 000 000 KGS/ сут. 200 000 USDT (Доллар США)/ сут. <i>(и эквивалент в других валютах)</i>

Для пользователей – физических лиц

Уровень верификации	Условия прохождения	Требования к документам	Способ передачи	Макс. лимит депозита	Макс. лимит вывода
Уровень 0 (верификация не пройдена)	Регистрация в Сервисе XRuby, подтверждение e-mail;	—	Подтверждение адреса e-mail посредством ввода временного одноразового OTP-кода, направленного на почту.	Пользователь вправе знакомиться с функционалом Сервиса. Возможность осуществления открытия Кошелька или совершения Сделок с использованием Сервиса недоступна.	Пользователь вправе знакомиться с функционалом Сервиса. Возможность осуществления открытия Кошелька или совершения Сделок с использованием Сервиса недоступна.
Уровень 1	Верификация номера мобильного телефона; Заполнение анкеты в Сервисе XRuby. Верификация Пользователя по паспорту, включая удалённую идентификацию.	1. Паспорт (ID-карта, водительское удостоверение или иной документ, предусмотренный для резидентов или нерезидентов); 2. Поверки Liveness с использованием сервиса SUMSUB TECH LTD; 3. Анкета физ. лица (встроенная в процесс регистрации).	Подтверждение номера телефона посредством ввода временного одноразового OTP-кода, направленного указанный в Сервисе XRuby телефон. Заполнение анкеты в Сервисе XRuby через личный кабинет, e-mail или мобильное приложение. Провождение поверки Liveness с исп-нием сервиса SUMSUB TECH LTD	Кыргызский сом - 5 000 000 KGS/сут. 60 000 USDT (Доллар США)/сут. <i>(и эквивалент в других валютах)</i>	Кыргызский сом - 2 500 000 KGS/сут. 30 000 USDT (Доллар США)/сут. <i>(и эквивалент в других валютах)</i>
Уровень 2	Подтверждение финансовой надёжности Пользователя в результате предоставления достоверной информации об источнике происхождения денежных средств (например, посредством предоставления выписки с банковского счета, договора купли-продажи или аренды и иных документов)		Предоставление документов с исп-нием сервиса SUMSUB TECH LTD	Кыргызский сом - 10 000 000 KGS/сут. 120 000 USDT (Доллар США)/сут. <i>(и эквивалент в других валютах)</i>	Кыргызский сом - 5 000 000 KGS/сут. 60 000 USDT (Доллар США)/сут. <i>(и эквивалент в других валютах)</i>

5. ПРОВЕРКА ОПЕРАЦИЙ И ПРИМЕНЕНИЕ ЦЕЛЕВЫХ САНКЦИЙ

5.1. Каждая Операция в Сервисе проходит предварительную проверку в соответствии с внутренними документами Оператора.

- 5.2. Оператор обязан безотлагательно заморозить Операции и (или) средства Пользователей, включённых в Санкционный перечень, без предварительного уведомления.
- 5.3. Оператор обязан незамедлительно приостановить Операции, в отношении которой принято решение о признании операции подозрительной.
- 5.4. Оператор вправе направлять запросы Пользователям, чьи Операции были приостановлены, на предоставление документов, подтверждающих законность проведения Операции.
- 5.5. В целях исполнения требований законодательства Кыргызской Республики в сфере противодействия легализации (отмыванию) преступных доходов и финансированию преступной деятельности Оператор разрабатывает, утверждает и внедряет Программу внутреннего контроля, являющуюся основным внутренним документом, регламентирующим деятельность по выявлению и предотвращению операций, связанных с легализацией (отмыванием) преступных доходов и финансированием преступной деятельности.
- 5.6. **Программа внутреннего контроля включает в себя следующие положения:**
- 5.6.1. Определение критериев и признаков подозрительных операций;
 - 5.6.2. Формирование перечня критериев и признаков, свидетельствующих о возможной связи операций с легализацией (отмыванием) преступных доходов либо финансированием преступной деятельности, в соответствии с требованиями законодательства Кыргызской Республики и рекомендациями уполномоченных государственных органов;
 - 5.6.3. Механизм выявления, документирования и анализа подозрительных операций;
 - 5.6.4. Установление порядка мониторинга, фиксации, документирования и последующего анализа операций, обладающих признаками подозрительности, с использованием автоматизированных и/или ручных методов контроля;
 - 5.6.5. Порядок действий персонала при обнаружении подозрительной активности;
 - 5.6.6. Определение алгоритма действий сотрудников Оператора при выявлении подозрительных операций, включая немедленное информирование ответственных лиц, оформление соответствующих внутренних сообщений и подготовку необходимых документов;
 - 5.6.7. Ведение журнала подозрительных операций и иной внутренней отчётности;
 - 5.6.8. Организация ведения специализированных журналов и иных форм внутренней отчетности по вопросам противодействия легализации (отмыванию) преступных доходов и финансированию преступной деятельности, обеспечивающих фиксацию и хранение информации о выявленных подозрительных операциях в сроки, установленные внутренними регламентами и законодательством Кыргызской Республики;
 - 5.6.9. Регламентация процедур предоставления информации о подозрительных операциях в уполномоченный государственный орган, а также определение сроков и форм взаимодействия с ГСФР в соответствии с требованиями действующего законодательства;
 - 5.6.10. Проведение регулярных внутренних проверок;
 - 5.6.11. Организация и проведение плановых и внеплановых внутренних проверок системы внутреннего контроля с целью оценки ее эффективности и своевременного выявления недостатков;
 - 5.6.12. Обучение сотрудников, ответственных за выполнение требований по противодействию легализации (отмыванию) преступных доходов и финансированию преступной деятельности;
 - 5.6.13. Обеспечение регулярного (не реже одного раза в год) обучения и повышения квалификации сотрудников, участвующих в реализации мероприятий по противодействию легализации (отмыванию) преступных доходов и финансированию преступной деятельности.
- 5.7. В соответствии с требованиями законодательства Кыргызской Республики в сфере противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов, под подозрительными операциями понимаются любые сделки, финансовые операции или иные действия клиента, которые по своему характеру, объему, частоте или иным обстоятельствам не соответствуют установленному профилю клиента, его обычной хозяйственной деятельности, финансовым возможностям или иным известным сведениям о клиенте. К числу подозрительных операций относятся, в частности, случаи, когда клиент осуществляет операции, объем или характер которых явно не соответствуют его профилю, либо когда наблюдается дробление крупных сумм на несколько мелких транзакций с целью обхода процедур обязательного контроля, а также ситуации, когда клиент предпринимает попытки уклониться от установленных процедур идентификации или предоставляет недостоверные сведения и документы. Кроме того, подозрительными считаются операции, связанные с источниками повышенного риска, включая взаимодействие с юрисдикциями, находящимися под санкциями или признанными недостаточно прозрачными с точки зрения ПФТД/ЛПД, а также с анонимными инструментами, такими как неидентифицированные электронные кошельки и иные аналогичные средства.

5.8. При выявлении признаков подозрительной операции комплаенс-офицер обязан незамедлительно зафиксировать соответствующую информацию во внутреннем журнале учета подозрительных операций, подробно указав дату и время выявления, обстоятельства, вызвавшие подозрение, а также все имеющиеся сведения об операции и клиенте. В случае, если характер операции требует приостановления ее исполнения в соответствии с внутренними процедурами и действующим законодательством, комплаенс-офицер принимает меры по временной блокировке операции до завершения необходимой внутренней проверки. В течение одного рабочего дня с момента выявления подозрительной операции комплаенс-офицер подготавливает и направляет в Государственную службу финансовой разведки Кыргызской Республики официальное уведомление в установленной форме, прилагая все необходимые документы и пояснения, подтверждающие основания для подозрений.

5.9. Вся информация, связанная с подозрительными операциями, подлежит строгой конфиденциальности, не может быть разглашена третьим лицам и используется исключительно в целях исполнения требований законодательства о ПФТД/ЛПД. Комплаенс-офицер и иные сотрудники, участвующие в выявлении и анализе подозрительных операций, защищены от какой-либо ответственности за добросовестное исполнение своих обязанностей по информированию уполномоченных органов, если их действия соответствуют внутренним регламентам и законодательству Кыргызской Республики.

6. КЛИЕНТЫ С ПОВЫШЕННЫМ УРОВНЕМ РИСКА И ПОЛИТИЧЕСКИ ЗНАЧИМЫЕ ЛИЦА (ПДЛ)

6.1. В соответствии с законодательством Кыргызской Республики в сфере противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов, к категории клиентов с повышенным уровнем риска относятся физические и юридические лица, чьи характеристики или деятельность объективно создают повышенную вероятность вовлечения в операции, связанные с легализацией преступных доходов или финансированием террористической деятельности. К данной категории относятся, в частности, политически значимые лица (ПДЛ), под которыми понимаются лица, занимающие или занимавшие в течение последних трех лет значимые государственные должности в Кыргызской Республике или иностранных государствах, включая руководителей высшего звена, депутатов, судей, а также их близких родственников и доверенных лиц. Кроме того, к клиентам повышенного риска причисляются нерезиденты, зарегистрированные в юрисдикциях, признанных международными организациями или уполномоченными органами Кыргызской Республики как офшорные зоны или территории с высоким уровнем риска отмывания преступных доходов, а также клиенты, систематически отказывающиеся предоставлять достоверную информацию, необходимую для идентификации, либо создающие искусственные препятствия в процессе верификации.

6.2. В отношении указанных категорий клиентов Оператор обязан применять усиленные меры контроля, включающие обязательное проведение углубленной проверки источников происхождения их средств и имущества с запросом документального подтверждения легальности доходов, а также установление особого порядка согласования операций таких клиентов с руководством Оператора или уполномоченным коллегиальным органом. Дополнительно вводится повышенная частота мониторинга операций данных клиентов – не реже одного раза в квартал, с обязательным анализом соответствия операций их деловому профилю. В случаях, когда комплексная оценка рисков выявляет обоснованные подозрения в возможном вовлечении клиента в операции, связанные с легализацией преступных доходов или финансированием террористической деятельности, Оператор вправе принять решение об отказе в установлении деловых отношений или их прекращении, с обязательным документальным обоснованием такого решения и уведомлением Государственной службы финансовой разведки Кыргызской Республики при наличии признаков подозрительных операций.

7. ХРАНЕНИЕ И ЗАЩИТА ИНФОРМАЦИИ

7.1. В целях обеспечения соответствия требованиям законодательства Кыргызской Республики в сфере противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов, Оператор устанавливает строгий порядок хранения и защиты всей информации, полученной в ходе идентификации клиентов, мониторинга их операций, а также документов, связанных с выявлением подозрительных операций. К числу таких документов относятся анкеты клиентов, копии удостоверяющих личность документов, результаты проверки бенефициарных владельцев, внутренние отчеты о подозрительных операциях, журналы учёта и иные формы документации, формируемые в процессе реализации Программы внутреннего контроля. Срок обязательного хранения указанных документов составляет не менее пяти лет с даты прекращения деловых отношений с клиентом или даты совершения последней операции, в зависимости от того, какой срок наступает позднее.

7.2. Хранение осуществляется преимущественно в электронном архиве, организованном с использованием специализированных защищённых программно-аппаратных комплексов, доступ к которым предоставляется исключительно уполномоченным сотрудникам, непосредственно ответственным за реализацию мер ПФТД/ЛПД. Оператор гарантирует комплексную защиту хранимой информации от несанкционированного доступа, копирования, модификации, уничтожения или иных форм неправомерного использования путём внедрения многоуровневой системы технических и организационных мер. К числу таких мер относятся строгое разграничение прав доступа на основе принципа минимальных привилегий, при

котором каждый сотрудник получает доступ только к данным, необходимым для исполнения его непосредственных должностных обязанностей; регулярное резервное копирование информации на географически распределённых защищённых носителях с целью предотвращения безвозвратной утраты данных в случае сбоев оборудования или форс-мажорных обстоятельств; обязательное использование сертифицированных средств криптографической защиты информации (шифрования) как при хранении данных, так и при их передаче по каналам связи; а также систематическое проведение аудита действий пользователей с фиксацией всех операций доступа к информации в специальных журналах безопасности для последующего анализа и выявления потенциальных инцидентов.

8. ВЗАИМОДЕЙСТВИЕ С УПОЛНОМОЧЕННЫМИ ОРГАНАМИ

8.1. В случае выявления подозрительной операции, а также при наступлении иных обстоятельств, подлежащих обязательному контролю в соответствии с законодательством Кыргызской Республики о противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов, Оператор, действующий через назначенного комплаенс-оффисера, обязан в установленном порядке направить соответствующее сообщение в Государственную службу финансовой разведки Кыргызской Республики. Направление сообщения осуществляется безотлагательно, но не позднее одного рабочего дня с момента выявления подозрительной операции или обстоятельства, подлежащего обязательному контролю.

8.2. Уведомление подготавливается в соответствии с требованиями и по формам, утвержденным нормативными правовыми актами Кыргызской Республики, с обязательным указанием всех предусмотренных сведений и приложением необходимых документов, подтверждающих основания для сообщения. Передача информации в ГСФР осуществляется с использованием официальных каналов связи, обеспечивающих целостность, сохранность и конфиденциальность передаваемых данных.

8.3. Все сведения о направленных в ГСФР сообщениях, а также принятые комплаенс-оффисером решения, фиксируются во внутреннем журнале учета подозрительных операций и иных событий, подлежащих обязательному контролю. Журнал ведётся в электронном или бумажном виде в соответствии с внутренними процедурами Оператора и хранится не менее установленного законодательством срока. Доступ к данным журналам предоставляется исключительно уполномоченным лицам, ответственным за реализацию мер по ПФТД/ЛПД, а также по запросу компетентных государственных органов в порядке, предусмотренном действующим законодательством Кыргызской Республики.