

ПРОГРАММА ВНУТРЕННЕГО КОНТРОЛЯ ОсОО "МАРТЕН ФИНАНС" ПО ПРОТИВОДЕЙСТВИЮ ФИНАНСИРОВАНИЮ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ И ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ

INTERNAL CONTROL PROGRAM OF MARTEN FINANCE LLC ON COUNTERING THE FINANCING OF CRIMINAL ACTIVITY AND THE LEGALIZATION (LAUNDERING) OF CRIMINAL PROCEEDS

ВВОДНАЯ ЧАСТЬ (ОБЩИЕ ПОЛОЖЕНИЯ)

1. INTRODUCTORY PART (GENERAL PROVISIONS)

1.1. Настоящая Программа внутреннего контроля ОсОО «Мартэн Файнэнс» по противодействию финансированию преступной деятельности и легализации (отмыванию) преступных доходов (далее – Программа) устанавливает комплекс мер, направленных на установление контроля и организацию мониторинга за обеспечением соблюдения требований законодательства Кыргызской Республики по вопросам противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов в ОсОО «Мартэн Файнэнс» (далее – Компания).

1.1. This Internal Control Program of Marten Finance LLC on countering the financing of criminal activity and the legalization (laundering) of criminal proceeds (hereinafter, the Program) establishes a set of measures aimed at establishing control and organizing monitoring to ensure compliance with the requirements of the legislation of the Kyrgyz Republic on countering the financing of criminal activity and the legalization (laundering) of criminal proceeds in Marten Finance LLC (hereinafter, the Company).

1.2. Настоящая Программа разработана в соответствии с:

1.2. This Program has been developed in accordance with:

- Законом КР «О противодействии финансированию преступной деятельности и легализации (отмыванию) преступных доходов» от 6 августа 2018 года № 87;

- the Law of the Kyrgyz Republic “On Countering the Financing of Criminal Activity and the Legalization (Laundering) of Criminal Proceeds” dated August 6, 2018 No. 87;

- Постановление Кабинета Министров Кыргызской Республики от 14 ноября 2025 года № 739 О мерах по реализации Закона Кыргызской Республики "О противодействии финансированию преступной деятельности и легализации (отмыванию) преступных доходов". Настоящая Программа разработана с учетом объемов и характера деятельности Компании на финансовом рынке на территории Кыргызской Республики в целях противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов (далее - с ПФПД ЛПД), и призвана способствовать в организации и осуществлении сотрудниками Компании мероприятий и процедур по выявлению, учету и предотвращению:

- the Resolution of the Cabinet of Ministers of the Kyrgyz Republic dated November 14, 2025 No. 739 “On measures for the implementation of the Law of the Kyrgyz Republic ‘On Countering the Financing of Criminal Activity and the Legalization (Laundering) of Criminal Proceeds’”.

This Program has been developed taking into account the scope and nature of the Company’s activities in the financial market in the territory of the Kyrgyz Republic for the purpose of countering the financing of criminal activity and the legalization (laundering) of criminal proceeds (hereinafter, CFCA/LCP), and is intended to assist in the organization and implementation by the Company’s employees of measures and procedures for the identification, recording, and prevention of:

- операций (сделок) с денежными средствами, иным имуществом, связанных с финансированием преступной деятельности и легализацией (отмыванием) преступных доходов;

- operations (transactions) with monetary funds and other property related to the financing of criminal activity and the legalization (laundering) of criminal proceeds;

- операций (сделок) необычного характера, вызывающих подозрение;

- operations (transactions) of an unusual nature giving rise to suspicion;

- операций (сделок) с повышенным уровнем риска с точки зрения ПФПД ЛПД

- operations (transactions) with an increased level of risk from the point of view of CFCA/LCP;

- participation of the Company’s employees in the financing of criminal activity and the legalization (laundering) of criminal proceeds or facilitation thereof;

- участия сотрудников Компании в осуществлении финансирования преступной деятельности и легализации (отмывании) преступных доходов или содействию;

- принятию адекватных решений при установлении деловых отношений с клиентами (а равно, контрагентами);

- проведению осмотрительной кадровой политики, обеспечению добросовестного и ответственного отношения сотрудников Компании к исполняемым функциям и должностным обязанностям, предотвращению коррупции персонала и его вовлечения в противоправную деятельность, связанную с финансированием пореступной деятельности и легализации (отмыванию) преступных доходов.

1.3. Основной целью внедрения программы является выработка системы мер, которые позволяют выявлять и предотвращать использование механизмов Компании для финансирования преступной деятельности и легализации (отмывания) преступных доходов, при осуществлении операций (сделок) с денежными средствами, производными финансовыми инструментами.

1.4. Основными задачами внутреннего контроля по ПФПД ЛПД является:

- своевременное выявление и фиксация признаков операций с денежными средствами, производными финансовыми инструментами, свидетельствующих о возможной подготовке и/или осуществлении операции по финансированию преступной деятельности и легализации (отмыванию) преступных доходов;

- осуществление мер по выявлению, оценке, мониторингу, управлению, снижению и документированию рисков;

- осуществление мер надлежащей проверки клиентов;

- применение целевых финансовых санкций и приостановление операций (сделок) при возникновении подозрений;

- применение мер в отношении Клиентов из высокорискованных стран;

- своевременное представление в орган финансовой разведки информации и документов, а также сообщений об операциях (сделках), подлежащих контролю и сообщению;

- обеспечение хранения сведений и документов об операциях (сделках), а также информации, полученной по результатам надлежащей проверки клиентов;

- обеспечение конфиденциальности сведений;

- making adequate decisions when establishing business relations with clients (as well as counterparties);

- conducting a prudent personnel policy, ensuring the conscientious and responsible attitude of the Company's employees toward the functions and official duties performed, preventing staff corruption and their involvement in unlawful activity related to the financing of criminal activity and the legalization (laundering) of criminal proceeds.

1.3. The main purpose of implementing the Program is to develop a system of measures that makes it possible to identify and prevent the use of the Company's mechanisms for the financing of criminal activity and the legalization (laundering) of criminal proceeds when carrying out operations (transactions) with monetary funds and derivative financial instruments.

1.4. The main objectives of internal control for CFCA/LCP are:

- timely identification and recording of signs of operations with monetary funds and derivative financial instruments indicating possible preparation and/or execution of an operation for the financing of criminal activity and the legalization (laundering) of criminal proceeds;

- implementation of measures for identifying, assessing, monitoring, managing, mitigating, and documenting risks;

- implementation of customer due diligence measures;

- application of targeted financial sanctions and suspension of operations (transactions) when suspicions arise;

- application of measures with respect to Clients from high-risk countries;

- timely submission to the financial intelligence authority of information and documents, as well as reports on operations (transactions) subject to control and reporting;

- ensuring the storage of information and documents on operations (transactions), as well as information obtained as a result of customer due diligence;

- ensuring confidentiality of information;

- ensuring fulfillment of other obligations provided for by the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

- обеспечение выполнения иных обязанностей, предусмотренных в законодательстве Кыргызской Республики в сфере ПФПД ЛПД.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Для целей настоящей Программы используются следующие понятия:

АРМ – специализированное программное обеспечение, позволяющее в автоматизированном режиме формировать и направлять сообщения об операциях (сделках) в орган финансовой разведки (ГСФР).

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

Бликие родственники - (родители, усыновители, усыновленные, полнородные и неполнородные братья и сестры, бабушка, дедушка, внуки, в отношении которых публичное должностное лицо несет финансовые затраты, в части покрытия расходов на проживание, образование, здравоохранение и другие необходимые расходы).

Верификация - процедура проверки идентификационных данных клиента и (или) бенефициарного владельца.

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 оффшорные зоны.

Выявление операций, подлежащих контролю и сообщению - этап организации внутреннего контроля Компании в целях ПФПД ЛПД, который включает определение операций, подлежащих контролю и сообщению в орган финансовой разведки в соответствии с требованиями нормативных правовых актов Кыргызской Республики.

Виртуальный актив - совокупность данных в электронно-цифровой форме, имеющая стоимость, являющаяся цифровым выражением ценности и/или средством удостоверения имущественных и/или неимущественных прав, которая создается, хранится и обращается с использованием технологии распределенных реестров или

2. TERMS AND DEFINITIONS

2.1. For the purposes of this Program, the following concepts are used:

ARM means specialized software that makes it possible, in an automated mode, to generate and send reports on operations (transactions) to the financial intelligence authority (SFRS).

Beneficial owner means an individual (individuals) who ultimately (through a chain of ownership and control), directly or indirectly (through third parties), owns the ownership right of a legal entity or controls the client, or the individual on whose behalf or in whose interest an operation (transaction) is performed.

Close relatives means parents, adoptive parents, adopted children, full and half brothers and sisters, grandfather, grandmother, grandchildren, in respect of whom a public official bears financial expenses in terms of covering accommodation, education, healthcare and other necessary expenses.

Verification means the procedure for checking the identification data of the client and/or the beneficial owner.

High-risk countries means states and territories (entities) that do not apply or insufficiently apply international standards on countering money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction, as well as offshore zones.

Identification of operations subject to control and reporting means a stage of organizing the Company's internal control for the purposes of CFCA/LCP, which includes determination of operations subject to control and reporting to the financial intelligence authority in accordance with the requirements of the regulatory legal acts of the Kyrgyz Republic.

Virtual asset means a set of data in electronic-digital form having value, being a digital expression of value and/or a means of certifying property and/or non-property rights, which is created, stored and circulated using distributed ledger technology or similar technology and is not a monetary unit (currency), means of payment or security.

IND means internal normative documents.

Business relations means relations between a client and a financial institution or between a client and a non-financial category of persons, arising on the basis of an agreement (oral or written) on the provision of services for carrying out an operation (transaction).

Freezing of an operation (transaction) and/or funds means prohibition of carrying out an operation (transaction) with monetary funds and/or financial

аналогичной технологии и не является денежной единицей (валютой), средством платежа и ценной бумагой.

ВНД – внутренние нормативные документы

Деловые отношения - отношения между клиентом и финансовым учреждением или клиентом и нефинансовой категорией лиц, возникшие на основе договоренности (устной или письменной) о предоставлении услуг по осуществлению операции (сделки).

Замораживание операции (сделки) и (или) средств - запрещение проведения операции (сделки) с денежными средствами и/или финансовыми инструментами или передачи, преобразования, отчуждения и перемещения любых финансовых активов;

Идентификация - процедура установления идентификационных данных о клиенте и (или) бенефициарном владельце.

Клиент - физическое или юридическое лицо (организация), иностранный траст или юридическое образование, принятые на обслуживание или находящиеся на обслуживании у финансового учреждения или нефинансовой категории лиц либо с которыми финансовое учреждение или нефинансовая категория лиц устанавливает или установила деловые отношения.

Легализация (отмывание) преступных доходов - придание правомерного вида владению, пользованию или распоряжению преступным доходом путем совершения любых действий (операций или сделок) по преобразованию (конверсии) или переводу имущества, если известно, что имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника происхождения имущества или оказания помощи лицу, участвующему в совершении преступления, с целью уклонения от ответственности за деяния; либо сокрытие или утаивание подлинного характера источника, местонахождения, способа распоряжения и перемещения имущества, а также прав на имущество или его принадлежность, если известно, что имущество представляет собой доходы от преступлений; либо сокрытие или непрерывное удержание имущества лицом, не участвовавшим в совершении преступления, если лицу известно, что имущество получено в результате совершения преступления; либо приобретение, владение или использование имущества, если в момент его получения лицу было известно, что имущество представляет собой доходы от преступлений.

Служба внутреннего контроля - уполномоченный сотрудник или структурное

instrument or transfer, conversion, alienation and movement of any financial assets.

Identification means the procedure for establishing identification data on a client and/or beneficial owner.

Client means an individual or legal entity (organization), a foreign trust or a legal arrangement accepted for servicing or being serviced by a financial institution or a non-financial category of persons, or with whom a financial institution or a non-financial category of persons establishes or has established business relations.

Legalization (laundering) of criminal proceeds means giving a lawful appearance to the possession, use or disposal of criminal proceeds by performing any actions (operations or transactions) for the transformation (conversion) or transfer of property, if it is known that the property constitutes proceeds from crimes, for the purpose of concealing or disguising the criminal source of origin of the property or assisting a person participating in the commission of a crime for the purpose of evading liability for the acts; or concealing or disguising the true nature of the source, location, method of disposal and movement of property, as well as rights to property or its ownership, if it is known that the property constitutes proceeds from crimes; or concealing or continuous retention of property by a person who did not participate in the commission of the crime, if the person knows that the property was obtained as a result of the commission of a crime; or acquisition, possession or use of property, if at the moment of its receipt the person knew that the property constituted proceeds from crimes.

Internal control service means an authorized employee or structural subdivision or the Company's compliance control service responsible for implementation of internal control programs for CFCA/LCP.

VA exchange operator means the Virtual Asset Exchange Operator.

Operations (transactions) means any operations (transactions) with funds performed for the establishment, change or termination of civil rights and obligations with funds.

Financial intelligence authority means the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic.

Virtual asset exchange operator means a virtual asset service provider providing services for the purchase and sale (exchange) of virtual assets and/or exchange between virtual assets on its own behalf.

Company means the Virtual Asset Exchange Operator.

подразделение либо служба комплаенс-контроля Компании, ответственные за осуществление программ внутреннего контроля по ПФПД ЛПД

Оператор обмена ВА – Оператор обмена виртуальных активов

Операции (сделки) - любые операции (сделки) со средствами, совершаемые для установления, изменения или прекращения гражданских прав и обязанностей со средствами.

Орган финансовой разведки - Государственная служба финансовой разведки при Министерстве финансов Кыргызской Республики.

Оператор обмена виртуальных активов - поставщик услуг виртуальных активов, предоставляющий услуги покупки и продажи (обмена) виртуальных активов и (или) обмена между виртуальными активами от своего имени.

Компания – Оператор обмена виртуальных активов

Комплаенс офицер (далее – КО) – в рамках настоящей Программы, ответственное лицо Компании, которое отвечает за осуществление программы внутреннего контроля в целях ПФПД ЛПД и представления сообщений в ГСФР.

Кошелек виртуального актива - средство (программное приложение или иной механизм/носитель) для хранения и перевода виртуального актива.

Подозрительная операция (сделка) - операция (сделка), подпадающая под следующие признаки:

а) если имеются подозрение или достаточные основания подозревать, что средства являются доходом, полученным преступным путем, в том числе от предикатных преступлений, или связаны с легализацией (отмыванием) преступных доходов;

б) если имеются подозрение или достаточные основания подозревать, что средства связаны с финансированием:

- террористов и экстремистов;
- террористических и экстремистских организаций (групп);
- террористической и экстремистской деятельности;
- организованных групп или преступных сообществ;
- распространением оружия массового уничтожения.

Подозрительная операция (сделка) определяется должностным лицом по ПФПД ЛПД в рамках законодательства в области ПФПД ЛПД для операций, совершаемых с

Compliance Officer (hereinafter, CO) means, within the framework of this Program, the responsible person of the Company who is responsible for implementation of the internal control program for the purposes of CFCA/LCP and submission of reports to the SFRS.

Virtual asset wallet means a means (software application or other mechanism/media) for storage and transfer of a virtual asset.

Suspicious operation (transaction) means an operation (transaction) falling under the following signs:

a) if there is suspicion or sufficient grounds to suspect that the funds are proceeds obtained by criminal means, including from predicate crimes, or are connected with legalization (laundering) of criminal proceeds;

b) if there is suspicion or sufficient grounds to suspect that the funds are connected with the financing of:

- terrorists and extremists;
- terrorist and extremist organizations (groups);
- terrorist and extremist activity;
- organized groups or criminal communities;
- proliferation of weapons of mass destruction.

A suspicious operation (transaction) is determined by the official for CFCA/LCP within the framework of legislation in the field of CFCA/LCP for operations performed with monetary funds and other property of the client and beneficial owner.

Criminal proceeds means income (funds) received or derived directly or indirectly as a result of commission of a crime in the territory of the Kyrgyz Republic or a foreign state.

Predicate crime (main crime) means any crime provided for by the criminal legislation of the Kyrgyz Republic or of a foreign state, as a result of the commission of which income (funds) was obtained, being the object (subject) of legalization (laundering) of criminal proceeds.

Public officials means one of the following individuals:

a) foreign public official means a person performing or having performed significant state or political functions (public functions) in a foreign state (heads of states or governments, senior officials in government, courts, armed forces, state bodies, enterprises or institutions, prominent political figures, including prominent figures of political parties);

b) national public official means a person occupying or having occupied a political and special state position or a political municipal position in the Kyrgyz Republic provided for by

денежными средствами, иным имуществом клиента и бенефициарного владельца.

Преступный доход - доход (средства), полученный или извлеченный прямо, или косвенно в результате совершения преступления на территории Кыргызской Республики или иностранного государства.

Предикатное преступление (основное преступление) - любое преступление, предусмотренное в уголовном законодательстве Кыргызской Республики или иностранного государства, в результате совершения которого получен доход (средства), являющийся объектом (предметом) легализации (отмывания) преступных доходов.

Публичные должностные лица - одно из следующих физических лиц:

а) 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, судах, вооруженных силах, государственных органах, предприятиях или учреждениях, видные политические деятели, в том числе видные деятели политических партий);

б) 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;

в) 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).

Приостановление - временный запрет на проведение операции (сделки) с денежными средствами и/или финансовыми инструментами.

Разовая операция (сделка) – операция (сделка), осуществляемая один раз при отсутствии

the Register of State and Municipal Positions of the Kyrgyz Republic approved by the President of the Kyrgyz Republic, as well as senior management of state corporations, prominent political figures, including prominent figures of political parties;

c) public official of an international organization means a senior official of an international organization to whom important functions have been or were entrusted by an international organization (heads, deputy heads and members of the board of an international organization or persons occupying equivalent positions in an international organization).

Suspension means a temporary prohibition on carrying out an operation (transaction) with monetary funds and/or financial instruments.

One-time operation (transaction) means an operation (transaction) carried out once in the absence of permanent business relations (contractual relations) between the client and the Company.

Unfreezing means cancellation of the prohibition on carrying out an operation (transaction) with funds and/or financial instruments or transfer, conversion, alienation and movement of any funds.

Risk-based approach means application of enhanced measures in the presence of a high level of risk, standard measures in the presence of a medium level of risk, or simplified measures in the presence of a low level of risk in accordance with the established risk management procedures (identification, assessment, monitoring, control, reduction of the degree of risk) (on the basis of the Regulation on customer due diligence approved by the Resolution of the Cabinet of Ministers of the Kyrgyz Republic dated November 14, 2025 No. 739, Chapter 3, paragraph 11, the concept of “medium risk” is introduced).

Consolidated Sanctions List of the Kyrgyz Republic (Sanctions List) means a list of individuals and legal entities, groups and organizations in respect of whom there is information on carrying out (committing) or participation in carrying out (committing) terrorist activity, extremist activity, proliferation of weapons of mass destruction, legalization (laundering) of criminal proceeds, creation and leadership of an organized group or criminal community for commission of crimes or participation in such group or community, or rendering other assistance to such group or community (hereinafter, criminal activity).

The Sanctions List includes:

a) the Consolidated Sanctions List of the Kyrgyz Republic;

b) the Consolidated Sanctions List of the UN Security Council.

постоянных деловых отношений (договорных отношений) между клиентом и Компанией.

Размораживание - отмена запрета на проведение операции (сделки) со средствами и/или финансовыми инструментами или передачу, преобразование, отчуждение и перемещение любых средств.

Риск-ориентированный подход - применение усиленных мер при наличии высокого уровня риска, стандартных мер при наличии среднего уровня риска или упрощенных мер при наличии низкого уровня риска в соответствии с установленными процедурами управления рисками (выявление, оценка, мониторинг, контроль, снижение степени риска) (на основании Положения о надлежащей проверке клиента, утвержденной постановлением Кабинета министров Кыргызской Республики от 14 ноября 2025 года № 739, глава 3 пункт 11. вводится понятие «средний риск»)

Сводный санкционный перечень Кыргызской Республики (Санкционный перечень) – перечень физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об осуществлении (совершении) или участии в осуществлении (совершении) террористической деятельности, экстремистской деятельности, распространении оружия массового уничтожения, легализации (отмывании) преступных доходов, создании и руководстве организованной группой или преступным сообществом для совершения преступлений или участия в данной группе или сообществе, или оказания иного содействия данной группе или сообществу (далее - преступная деятельность).

Санкционный перечень включает в себя:

a) сводный санкционный перечень Кыргызской Республики;

b) сводный санкционный перечень Совета Безопасности ООН.

c) Перечень высоко рисковых стран

Порядок формирования и опубликования санкционного перечня предусмотрен в Положении "О перечнях физических лиц и юридических лиц, групп и организаций, в отношении которых имеются сведения об их участии в террористической и экстремистской деятельности, распространении оружия массового уничтожения и легализации (отмывании) преступных доходов", утвержденном постановлением Кабинета министров Кыргызской Республики от 14 ноября 2025 года № 739 О мерах по реализации Закона Кыргызской Республики "О противодействии финансированию преступной

c) list of high-risk countries

The procedure for formation and publication of the Sanctions List is provided for in the Regulation "On Lists of Individuals and Legal Entities, Groups and Organizations in Respect of Whom There Is Information on Their Participation in Terrorist and Extremist Activity, Proliferation of Weapons of Mass Destruction and Legalization (Laundering) of Criminal Proceeds," approved by the Resolution of the Cabinet of Ministers of the Kyrgyz Republic dated November 14, 2025 No. 739 "On Measures for the Implementation of the Law of the Kyrgyz Republic 'On Countering the Financing of Criminal Activity and the Legalization (Laundering) of Criminal Proceeds.'"

Funds means one of the following assets:

a) monetary funds and any financial assets, including virtual assets;

b) economic resources, including oil and other natural resources;

c) property of any kind (material or immaterial, movable or immovable), regardless of the method of acquisition;

d) legal documents or instruments in any form, including electronic or digital form, granting the right or share to the above-mentioned property or assets;

e) bank loans and monetary funds and/or other property received/issued in accordance with Islamic principles of banking and finance, money and settlement checks, postal transfers, shares, securities, bonds, bank drafts or letters of credit and any interest, dividends and income received from or generated by such funds or assets.

Structural subdivision means a directorate, department, branch and other separate subdivisions of the Company.

Accounts means accounts, or analogous business relations between a financial institution and a client or between a non-financial category of persons and a client.

FATCA (Foreign Account Tax Compliance Act) means the law on tax reporting on foreign accounts (hereinafter, the FATCA Law), which is aimed against tax evasion by residents of the United States of America. The FATCA Law obliges foreign financial organizations to report to the IRS on the movement of funds of US taxpayers.

FATF means an intergovernmental organization (group) for the development and implementation of international standards on combating money laundering and terrorist financing.

Financing of criminal activity means financing of terrorist activity, financing of extremist activity, financing of proliferation of weapons of mass destruction, financing of organized groups or criminal communities.

деятельности и легализации (отмыванию) преступных доходов".

Средства - одно из следующих активов:

- a) денежные средства и любые финансовые активы, в том числе виртуальные активы;
- b) экономические ресурсы, включая нефть и другие природные ресурсы;
- c) имущество любого вида (материальное или нематериальное, движимое или недвижимое) независимо от способа приобретения;
- d) правовые документы или инструменты в любой форме, в том числе в электронной или цифровой, предоставляющие право или долю на вышеуказанное имущество или активы;
- e) банковские кредиты и денежные средства и (или) иное имущество, получаемые/выдаваемые в соответствии с исламскими принципами банковского дела и финансирования, денежные и расчетные чеки, почтовые переводы, акции, ценные бумаги, облигации, банковские тратты или аккредитивы и любые проценты, дивиденды и доход, получаемые от таких средств или активов или производимые ими.

Структурное подразделение – управление, отдел, филиал и другие обособленные подразделения Компании.

Счета - счета, или аналогичные деловые отношения между финансовым учреждением и клиентом или между нефинансовой категорией лиц и клиентом.

FATCA (анг. - Foreign Account Tax Compliance Act) – Закон о налоговой отчетности по зарубежным счетам (далее – Закон FATCA), который направлен против уклонения резидентов Соединенных Штатов Америки от уплаты налогов. Закон FATCA обязывает иностранные финансовые организации отчитываться перед IRS о движении средств налогоплательщиков США.

ФАТФ – межправительственная организация (группа) по разработке и внедрению международных стандартов по борьбе с отмыванием денег и финансированием терроризма.

Финансирование преступной деятельности - финансирование террористической деятельности, финансирование экстремистской деятельности, финансирование распространения оружия массового уничтожения, финансирование организованных групп или преступных сообществ.

Финансирование распространения оружия массового уничтожения - предоставление или

Financing of proliferation of weapons of mass destruction means provision or collection of funds or rendering of financial services with awareness that the funds are intended or will be used in whole or in part to finance the proliferation of nuclear, chemical and biological weapons and/or their means of delivery.

Targeted financial sanctions means freezing of any operations (transactions) and/or funds of individuals and legal entities, groups and organizations included in the Sanctions List, and/or restriction of granting such persons, groups and organizations access (direct or indirect) to any funds or financial services.

Electronic money transfer means an operation for the transfer of funds (cash, non-cash funds, electronic money) from the sender to the recipient of the money transfer carried out using payment systems.

Legal arrangements means trust funds and other similar legal relations for management and disposal of property created in accordance with the legislation of a foreign state.

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;

Целевые финансовые санкции - замораживание любых операций (сделок) и (или) средств физических и юридических лиц, групп и организаций, включенных в Санкционный перечень, и (или) ограничение предоставления таким лицам, группам и организациям доступа (прямого или косвенного) к любым средствам или финансовым услугам.

Электронный денежный перевод - операция по переводу денежных средств (наличных, безналичных, электронных денег) от отправителя к получателю денежного перевода, осуществляемая с использованием платежных систем.

Юридические образования - доверительные фонды и другие аналогичные юридические отношения по управлению и распоряжению имуществом, создаваемые в соответствии с законодательством иностранного государства.

3. ПОРЯДОК ПРОВЕРКИ СОТРУДНИКОВ ПРИ ПРИЕМЕ (НАЙМЕ) НА РАБОТУ

3.1. Оператор обмена виртуальных активов при приеме (найме) на работу сотрудников обязан потребовать и проверить документы лица, поступающего на работу (кандидата) в соответствии с Трудовым Кодексом Кыргызской Республики: документ, удостоверяющий личность, трудовую книжку, персональный идентификационный номер, а также документы воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу), и документ об образовании; справку о несудимости, а также дополнительные документы с учетом специфики выполняемой работы в соответствии с Трудовым Кодексом, законами в сфере виртуальных активов, законодательством в сфере ПФПД ЛПД.

3.2. Оператор обмена виртуальных активов проводит проверку кандидата на наличие или отсутствие судимости, путем запроса справки об отсутствии судимости из органов внутренних дел, а также проверку на наличие или отсутствие в национальном и международном списках разыскиваемых лиц и перечнях физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об участии в преступной

3. PROCEDURE FOR CHECKING EMPLOYEES UPON HIRING (EMPLOYMENT)

3.1. When hiring employees, the virtual asset exchange operator is obliged to request and verify the documents of the person applying for employment (candidate) in accordance with the Labor Code of the Kyrgyz Republic: an identity document, employment record book, personal identification number, as well as military registration documents (for persons liable for military service and persons subject to military conscription), and an education document; a certificate of no criminal record, as well as additional documents taking into account the specifics of the work performed in accordance with the Labor Code, laws in the field of virtual assets, and legislation in the field of CFCA/LCP.

3.2. The virtual asset exchange operator checks the candidate for the presence or absence of a criminal record by requesting a certificate of no criminal record from the internal affairs bodies, as well as checking for presence or absence in national and international wanted persons lists and in the lists of individuals and legal entities, groups and organizations in respect of whom there is information about participation in criminal activity and the legalization (laundering) of criminal proceeds, using the official websites of Interpol, the internal affairs body, the national security body and the financial intelligence authority of the Kyrgyz Republic.

деятельности и легализации (отмывании) преступных доходов, с использованием официальных сайтов Интерпола, органа внутренних дел, органа национальной безопасности и органа финансовой разведки Кыргызской Республики.

3.3. Оператор обмена виртуальных активов хранит результаты проверки лица, поступающего на работу и документы в Личном досье сотрудника.

4. ПОРЯДОК ОПРЕДЕЛЕНИЯ СЛУЖБЫ ВНУТРЕННЕГО КОНТРОЛЯ

4.1. Служба внутреннего контроля Оператора обмена ВА создается с учетом особенностей деятельности, штатной численности, клиентской базы и уровня рисков. При штатной численности сотрудников до трех человек Оператор обмена ВА возлагает функции службы внутреннего контроля на Директора. При увеличении штатной численности сотрудников свыше трех человек, в Компании решением Учредителей/Участников создается Служба внутреннего контроля. Руководитель службы внутреннего контроля по статусу находится на уровне руководителя (заместителя руководителя) Компании.

4.2. Руководитель и сотрудники службы внутреннего контроля назначаются на должность и освобождаются от должности решением руководителя Оператора обмена ВА по согласованию с высшим органом управления.

4.3. Руководитель службы внутреннего контроля подотчетен непосредственно высшему органу управления Оператора обмена ВА. Сотрудники службы внутреннего контроля подотчетны непосредственно руководителю службы внутреннего контроля.

4.4. Сотрудники Оператора обмена ВА оказывают содействие службе внутреннего контроля в осуществлении функций службы внутреннего контроля согласно данной Программе внутреннего контроля по ПФПД ЛПД, а также другими внутренними нормативными документами Компании по ПФПД ЛПД, а также должностными инструкциями.

4.5. При приеме на работу в службу внутреннего контроля к кандидату предъявляются следующие квалификационные требования:

- 1) высшее образование;
- 2) знание законодательства Кыргызской Республики в сфере ПФПД ЛПД;

3.3. The virtual asset exchange operator keeps the results of the check of the person applying for employment and the documents in the employee's Personal File.

4. PROCEDURE FOR DETERMINING THE INTERNAL CONTROL SERVICE

4.1. The Internal Control Service of the VA Exchange Operator is created taking into account the specifics of the activity, staff headcount, client base and risk level. If the staff headcount is up to three persons, the VA Exchange Operator assigns the functions of the internal control service to the Director. If the staff headcount exceeds three persons, the Company creates an Internal Control Service by decision of the Founders/Participants. The head of the internal control service has a status at the level of the head (deputy head) of the Company.

4.2. The head and employees of the internal control service are appointed and dismissed by decision of the head of the VA Exchange Operator in agreement with the highest management body.

4.3. The head of the internal control service is directly accountable to the highest management body of the VA Exchange Operator. Employees of the internal control service are directly accountable to the head of the internal control service.

4.4. Employees of the VA Exchange Operator provide assistance to the internal control service in carrying out the functions of the internal control service according to this Internal Control Program for CFCA/LCP, as well as other internal normative documents of the Company on CFCA/LCP, and also job descriptions.

4.5. When hiring into the internal control service, the following qualification requirements apply to the candidate:

- 1) higher education;
- 2) knowledge of the legislation of the Kyrgyz Republic in the field of CFCA/LCP;
- 3) knowledge of risks characteristic of the activities of a virtual asset exchange operator.

4.6. The head and employees of the internal control service are independent in their actions. The internal control service ensures control over the compliance of operations (transactions) carried out with the requirements of the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

4.7. The objectives of the internal control service are:

- 1) exclusion of the involvement of the VA Exchange Operator and participation of its

3) знание о рисках, характерных для деятельности Оператора обмена виртуальных активов.

4.6. Руководитель и сотрудники службы внутреннего контроля независимы в своих действиях. Служба внутреннего контроля обеспечивает контроль за соответствием проводимых операций (сделок) требованиям законодательства Кыргызской Республики в сфере ПФПД ЛПД.

4.7. Задачами службы внутреннего контроля являются:

1) исключение вовлечения Оператора обмена ВА и участия его работников в совершении преступных (незаконных) деяний;

2) эффективная реализация законодательства Кыргызской Республики в сфере ПФПД ЛПД;

3) содействие органу финансовой разведки и проверяющим органам в выполнении задач и функций, предусмотренных законодательством Кыргызской Республики в сфере ПФПД ЛПД.

4.8. Служба внутреннего контроля выполняет следующие функции:

1) разработка и представление высшему органу управления Оператора обмена ВА проектов программ внутреннего контроля и иных внутренних документов в сфере ПФПД ЛПД, в том числе методологии оценки рисков и процедур управления рисками;

2) реализация программ внутреннего контроля;

3) мониторинг проведения надлежащей проверки клиента и иных участников операций (сделок);

4) мониторинг и анализ операций (сделок) клиента;

5) принятие решения о признании операции (сделки) подозрительной и направлении сообщения о подозрительной операции (сделке) в орган финансовой разведки с последующим уведомлением исполнительного органа;

6) представление в орган финансовой разведки сообщений об операциях (сделках), подлежащих контролю и сообщению, в соответствии с законодательством Кыргызской Республики в сфере ПФПД ЛПД;

7) оказание содействия уполномоченным представителям проверяющих органов при проведении ими проверки деятельности Оператора обмена ВА по вопросам соблюдения законодательства Кыргызской Республики в сфере ПФПД ЛПД;

8) представление высшему органу управления Оператора обмена ВА ежеквартального письменного отчета о результатах реализации программ внутреннего контроля.

employees in the commission of criminal (illegal) acts;

2) effective implementation of the legislation of the Kyrgyz Republic in the field of CFCA/LCP;

3) assistance to the financial intelligence authority and supervisory authorities in carrying out tasks and functions provided for by the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

4.8. The internal control service performs the following functions:

1) development and submission to the highest management body of the VA Exchange Operator of drafts of internal control programs and other internal documents in the field of CFCA/LCP, including risk assessment methodology and risk management procedures;

2) implementation of internal control programs;

3) monitoring of the conduct of customer due diligence and other participants in operations (transactions);

4) monitoring and analysis of client operations (transactions);

5) making a decision on recognizing an operation (transaction) as suspicious and sending a report on a suspicious operation (transaction) to the financial intelligence authority with subsequent notification of the executive body;

6) submission to the financial intelligence authority of reports on operations (transactions) subject to control and reporting, in accordance with the legislation of the Kyrgyz Republic in the field of CFCA/LCP;

7) assistance to authorized representatives of supervisory authorities when they carry out inspections of the activities of the VA Exchange Operator on issues of compliance with the legislation of the Kyrgyz Republic in the field of CFCA/LCP;

8) submission to the highest management body of the VA Exchange Operator of a quarterly written report on the results of implementation of internal control programs.

4.9. The internal control service has the right to:

1) receive the necessary administrative and accounting documents of the VA Exchange Operator;

2) receive access to databases of clients and beneficial owners formed by the VA Exchange Operator;

3) in the established manner, enter the premises of the divisions of the VA Exchange Operator, as well as premises used for storing documents (archives), cash and valuables (cash vaults), and the information database;

4) receive and make copies of the necessary documents, electronic files and records stored in

4.9. Служба внутреннего контроля имеет право:

- 1) получать необходимые распорядительные и бухгалтерские документы Оператора обмена ВА;
- 2) получать доступ к базам данных клиентов и бенефициарных владельцев, формируемым Оператором обмена ВА;
- 3) в установленном порядке входить в помещения подразделений Оператора обмена ВА, а также в помещения, используемые для хранения документов (архивы), наличных денег и ценностей (денежные хранилища), информационной базы данных;
- 4) получать и снимать копии с необходимых документов, электронных файлов и записей, хранящихся в информационных системах Оператора обмена ВА;
- 5) давать временные указания, касающиеся проведения операции (сделки), в том числе предписания о приостановлении операции (сделки) и замораживании операции (сделки) и (или) средств;
- 6) совершать иные действия в соответствии с внутренними документами Оператора обмена ВА.

4.10. Служба внутреннего контроля обязана:

- 1) обеспечивать сохранность и возврат полученных документов Оператора обмена ВА;
- 2) соблюдать конфиденциальность информации, полученной при осуществлении своих функций, и не разглашать данные при передаче информации органу финансовой разведки;
- 3) совершать иные действия в соответствии с внутренними документами Оператора обмена ВА.

4.11. Сотрудники Оператора обмена обязаны оказать содействие службе внутреннего контроля в осуществлении ее функций в соответствии с настоящей Программой внутреннего контроля по ПФПД ЛПД и внутренними нормативными документами по ПФПД ЛПД, а также должностными инструкциями.

4.12. Сотрудники Оператора обмена ВА, которым стали известны факты нарушений законодательства Кыргызской Республики в сфере ПФПД ЛПД, совершенных в Компании, в течение одного рабочего дня в письменном виде обязаны довести эти факты до сведения своего непосредственного руководителя и службы внутреннего контроля.

the information systems of the VA Exchange Operator;

- 5) give temporary instructions relating to the carrying out of an operation (transaction), including orders on suspension of an operation (transaction) and freezing of an operation (transaction) and/or funds;
- 6) perform other actions in accordance with the internal documents of the VA Exchange Operator.

4.10. The internal control service is obliged to:

1. ensure the safekeeping and return of the received documents of the VA Exchange Operator;
2. maintain confidentiality of information obtained in the course of carrying out its functions and not disclose data when transmitting information to the financial intelligence authority;
3. perform other actions in accordance with the internal documents of the VA Exchange Operator.

4.11. Employees of the Exchange Operator are obliged to provide assistance to the internal control service in carrying out its functions in accordance with this Internal Control Program for CFCA/LCP and internal normative documents on CFCA/LCP, as well as job descriptions.

4.12. Employees of the VA Exchange Operator who become aware of facts of violations of the legislation of the Kyrgyz Republic in the field of CFCA/LCP committed in the Company shall, within one working day, notify their immediate supervisor and the internal control service of these facts in writing.

5. ПОРЯДОК УСТАНОВЛЕНИЯ ОТНОШЕНИЙ ОПЕРАТОРА ВИРТУАЛЬНЫХ АКТИВОВ

5.1. Оператор обмена виртуальных активов вправе устанавливать отношения с другими поставщиками услуг виртуальных активов, которыми могут выступать юридические лица (как резиденты, так и нерезиденты Кыргызской Республики), после проведения комплексной проверки контрагента, включая оценку рисков контрагента. Перед началом сотрудничества Оператор обмена обязан убедиться в благонадежности партнера: проверить наличие регистрации и лицензии у контрагента в его юрисдикции, провести анализ внутренних политик партнера по ПФПД ЛПД, проверить обязательность передачи и получения информации об отправителе и получателе при переводах активов между Оператором обмена и контрагентом. Оператор обмена обязан учесть риски юрисдикции: при оценке контрагента учитывать «страновой риск», то есть риски установления деловых отношений с клиентом из высоко рискованной страны, согласно законодательства Кыргызской Республики в сфере ПФПД ЛПД, произвести проверку отсутствия контрагента и его юрисдикции в санкционных перечнях определенных законодательством Кыргызской Республики в сфере ПФПД ЛПД. Контрагенты лицензируемые ПУВА, как профессиональные участники рынка виртуальных активов, берут все возможные риски при операциях с виртуальными активами на себя, и в их отношении Оператор обмена виртуальных активов не проводит тесты на знание виртуальных активов.

5.2. Оператор обмена виртуальных активов вправе устанавливать отношения с клиентами, которыми могут выступать любые физические и юридические лица (как резиденты, так и нерезиденты Кыргызской Республики), за исключением случаев, предусмотренных законодательством Кыргызской Республики, в сфере противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов.

5.3. Отношения оператора обмена виртуальных активов с клиентами строятся на договорной основе.

5.4. В договорах, посредством которых устанавливаются отношения с клиентами, оператор обмена виртуальных активов обязан предусматривать условия, предусмотренные Положением о деятельности оператора обмена виртуальных активов и ведении Реестра операторов обмена виртуальных активов, а

5. PROCEDURE FOR ESTABLISHING RELATIONS OF THE VIRTUAL ASSET OPERATOR

5.1. The virtual asset exchange operator has the right to establish relations with other virtual asset service providers, which may be legal entities (both residents and non-residents of the Kyrgyz Republic), after conducting comprehensive due diligence of the counterparty, including assessment of the counterparty's risks. Before the start of cooperation, the Exchange Operator is obliged to make sure of the partner's reliability: verify the presence of registration and license of the counterparty in its jurisdiction, conduct an analysis of the partner's internal CFCA/LCP policies, verify the obligation to transmit and receive information about the sender and recipient in asset transfers between the Exchange Operator and the counterparty. The Exchange Operator is obliged to take into account jurisdiction risks: when assessing the counterparty, take into account the "country risk," that is, the risks of establishing business relations with a client from a high-risk country, according to the legislation of the Kyrgyz Republic in the field of CFCA/LCP, and verify the absence of the counterparty and its jurisdiction in the sanctions lists determined by the legislation of the Kyrgyz Republic in the field of CFCA/LCP. Counterparties that are licensed VASPs, as professional participants of the virtual assets market, assume all possible risks in transactions with virtual assets, and in their respect the virtual asset exchange operator does not conduct tests on knowledge of virtual assets.

5.2. The virtual asset exchange operator has the right to establish relations with clients, who may be any individuals and legal entities (both residents and non-residents of the Kyrgyz Republic), except for cases provided for by the legislation of the Kyrgyz Republic in the field of countering the financing of criminal activity and legalization (laundering) of criminal proceeds.

5.3. The relations of the virtual asset exchange operator with clients are built on a contractual basis.

5.4. In the contracts through which relations with clients are established, the virtual asset exchange operator is obliged to provide for the conditions stipulated by the Regulation on the activities of the virtual asset exchange operator and maintenance of the Register of virtual asset exchange operators, as well as by the Law of the Kyrgyz Republic "On Virtual Assets."

5.5. To establish relations with a client, the virtual asset exchange operator requests from him the following information:

также Законом Кыргызской Республики "О виртуальных активах".

5.5. Для установления отношений с клиентом оператор обмена виртуальных активов запрашивает у него следующую информацию:

- у физического лица - фамилию, собственное имя, отчество (если таковое имеется), дату рождения, адрес места жительства, согласно паспорту или документу, удостоверяющего личность;
- у юридического лица - наименование, место нахождения, идентификационный номер плательщика, согласно свидетельству о государственной регистрации юридического лица;
- контактные данные клиента, позволяющие установить с ним связь (адрес электронной почты и при необходимости иные контактные данные);
- сведения, предусмотренные локальными актами или договорными обязательствами оператора обмена виртуальных активов, в том числе в сфере предотвращения легализации доходов, полученных преступным путем, финансирования преступной деятельности и финансирования распространения оружия массового поражения.

5.6. В случае, если оператор обмена виртуальных активов предоставляет клиентам возможность создания электронного личного кабинета на своей платформе, оператор обмена виртуальных активов обязан принимать меры по исключению создания одним и тем же клиентом двух и более электронных личных кабинетов.

5.7. Оператор обмена виртуальных активов не вправе устанавливать отношения с:

- физическими лицами, не достигшими 18 лет;
- нерезидентами Кыргызской Республики, если это противоречит законодательству государства, гражданами (подданными) которого являются нерезиденты Кыргызской Республики и (или) на территории которого они имеют постоянное место жительства в соответствии с видом на жительство (или аналогичным документом) либо место нахождения (учреждены, зарегистрированы);
- физическими лицами, индивидуальными предпринимателями, юридическими лицами, а также юридическими лицами, бенефициарные владельцы, которых включены в санкционный перечень, определенный законодательством в сфере противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов, а также противодействия финансированию

from an individual – surname, first name, patronymic (if any), date of birth, residential address, according to the passport or identity document;

from a legal entity – name, location, taxpayer identification number, according to the certificate of state registration of the legal entity;

the client's contact details allowing contact with him to be established (email address and, if necessary, other contact details);

information provided for by local acts or contractual obligations of the virtual asset exchange operator, including in the field of prevention of legalization of proceeds obtained by criminal means, financing of criminal activity and financing of the proliferation of weapons of mass destruction.

5.6. If the virtual asset exchange operator provides clients with the possibility of creating an electronic personal account on its platform, the virtual asset exchange operator is obliged to take measures to prevent the same client from creating two or more electronic personal accounts.

5.7. The virtual asset exchange operator is not entitled to establish relations with:

- individuals under the age of 18;
- non-residents of the Kyrgyz Republic, if this contradicts the legislation of the state of which the non-residents of the Kyrgyz Republic are citizens (subjects) and/or in whose territory they have a permanent place of residence in accordance with a residence permit (or similar document) or location (are established, registered);
- individuals, individual entrepreneurs, legal entities, as well as legal entities whose beneficial owners are included in the sanctions list determined by legislation in the field of countering the financing of criminal activity and legalization (laundering) of criminal proceeds, as well as countering the financing of extremist activity and financing of the proliferation of weapons of mass destruction;
- other persons, if this is provided for by contractual obligations of the virtual asset exchange operator or local acts of the virtual asset exchange operator.

5.8. Before carrying out transactions with citizens of the Kyrgyz Republic for the sale of virtual assets to them for money or electronic money, the virtual asset exchange operator is obliged to make sure that they possess a sufficient level of knowledge (competence) to carry out such transactions. The virtual asset exchange operator is not entitled to carry out the said transactions with those citizens of the Kyrgyz Republic in respect of whom it has established that they do not possess such a level of knowledge (competence).

экстремистской деятельности и финансированию распространения оружия массового уничтожения;

- иными лицами, если это предусмотрено, договорными обязательствами оператора обмена виртуальных активов или локальными актами оператора обмена виртуальных активов.

5.8. До совершения с гражданами Кыргызской Республики сделок по продаже им виртуальных активов за деньги или электронные деньги оператор обмена виртуальных активов обязан убедиться в том, что они обладают достаточным уровнем знаний (компетентности) для совершения таких сделок. Оператор обмена виртуальных активов не вправе совершать названные сделки с теми гражданами Кыргызской Республики, в отношении которых он установил, что они таким уровнем знаний (компетентности) не обладают.

5.9. Определение уровня знаний (компетентности) для совершения сделок, указанных в части первой настоящего пункта, производится оператором обмена виртуальных активов посредством представления гражданам Кыргызской Республики вопросника (теста) для заполнения (решения).

5.10. Оператор обмена виртуальных активов обязан обеспечить хранение документов по идентификации клиента (анкета клиента), договора, если клиент юридическое лицо, учредительных документов, свидетельства о регистрации, а также документов, полученных в ходе определения уровня знаний (компетентности), предусмотренного в части четвертой, не менее 5 календарных лет с даты получения таких документов.

5.11. Оператор обмена виртуальных активов вправе самостоятельно определить критерии, которым должны соответствовать нерезиденты Кыргызской Республики, а также юридические лица Кыргызской Республики для установления с ними отношений (в том числе требования к финансовому состоянию и репутации). При этом установленные критерии должны соответствовать требованиям законодательства Кыргызской Республики в части противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов.

5.12. Оператор обмена виртуальных активов обязан:

- производить звукозапись (видеозапись) переговоров с клиентами, осуществляемых с использованием средств связи (с обязательным предварительным уведомлением об этом клиента);

5.9. Determination of the level of knowledge (competence) for carrying out the transactions specified in part one of this paragraph is carried out by the virtual asset exchange operator by means of providing citizens of the Kyrgyz Republic with a questionnaire (test) to be filled out (solved).

5.10. The virtual asset exchange operator is obliged to ensure storage of documents for client identification (client questionnaire), the contract, if the client is a legal entity, constituent documents, certificate of registration, as well as documents obtained in the course of determining the level of knowledge (competence) provided for in part four, for at least 5 calendar years from the date of receipt of such documents.

5.11. The virtual asset exchange operator has the right to independently determine the criteria that non-residents of the Kyrgyz Republic, as well as legal entities of the Kyrgyz Republic, must meet in order to establish relations with them (including requirements for financial condition and reputation). At the same time, the established criteria must comply with the requirements of the legislation of the Kyrgyz Republic in terms of countering the financing of criminal activity and legalization (laundering) of criminal proceeds.

5.12. The virtual asset exchange operator is obliged to:

- make audio recordings (video recordings) of negotiations with clients carried out using means of communication (with mandatory prior notification of the client thereof);

- store audio recording (video recording) data and all correspondence with clients for at least 5 calendar years from the date of making (occurrence of) such audio recordings (video recordings) and correspondence;

- perform backup copying of all data on transactions (operations) made by clients at the end of each working day;

- ensure immediate execution of clients' applications for the purchase and/or sale of virtual assets for money or electronic money or exchange of one type of virtual assets for another type of virtual assets in accordance with this Regulation (if it is possible to execute such applications);

- take measures to ensure knowledge by employees of the virtual asset exchange operator and persons engaged by it under civil law contracts, who are directly involved in carrying out the activities of the virtual asset exchange operator, of the law in the field of circulation of virtual assets, its local normative legal acts, as well as the Regulation on the activities of the virtual asset exchange operator and maintenance of the Register of virtual asset exchange operators;

- хранить данные звукозаписи (видеозаписи) и всю переписку с клиентами в течение не менее 5 календарных лет с даты осуществления (возникновения) таких звукозаписей (видеозаписей) и переписки;
- осуществлять резервное копирование всех данных о совершенных клиентами сделках (операциях) по завершении каждого рабочего дня;
- обеспечивать незамедлительное исполнение заявок клиентов на покупку и (или) продажу виртуальных активов за деньги или электронные деньги либо обмен виртуальных активов одного вида на виртуальные активы другого вида в соответствии с настоящим Положением (при наличии возможности исполнить такие заявки);
- принимать меры по обеспечению знания работниками оператора обмена виртуальных активов и лицами, привлеченными им по гражданско-правовым договорам, которые непосредственно вовлечены в осуществление деятельности оператора обмена виртуальных активов, законом в сфере оборота виртуальных активов, его локальных нормативных правовых актов, а также Положения о деятельности оператора обмена виртуальных активов и ведении Реестра операторов обмена виртуальных активов;
- выполнять другие требования, предусмотренные Законом Кыргызской Республики "О виртуальных активах", а также Положением о деятельности оператора обмена виртуальных активов и ведении Реестра операторов обмена виртуальных активов.

- comply with other requirements provided for by the Law of the Kyrgyz Republic "On Virtual Assets," as well as by the Regulation on the activities of the virtual asset exchange operator and maintenance of the Register of virtual asset exchange operators.

6. НАДЛЕЖАЩАЯ ПРОВЕРКА КЛИЕНТА KYC (Знай Своего Клиента)

6.1. Случаи осуществления надлежащей проверки клиентов.

6.1.1. Учредители Компании утверждают внутренние нормативные документы, в которых подробно определен порядок проведения надлежащей проверки клиентов.

6.2. Компанией проводится надлежащая проверка клиентов (в рамках реализуемой политики Знай Своего Клиента) **на основе риск-ориентированного подхода** в любом из следующих случаев:

- при установлении деловых отношений;
- при совершении разовой операции (сделки) или нескольких взаимосвязанных разовых операций (сделок) по купле-продаже (обмену) наличной национальной и/или иностранной валют на сумму, равную или превышающую 1 000 000 сомов или эквивалента в иностранной валюте;

6. CUSTOMER DUE DILIGENCE KYC (KNOW YOUR CUSTOMER)

6.1. Cases of conducting customer due diligence.

6.1.1. The Founders of the Company approve internal normative documents in which the procedure for conducting customer due diligence is defined in detail.

6.2. The Company conducts appropriate customer due diligence (as part of its Know Your Customer policy) using **a risk-based approach** in any of the following cases:

- upon establishment of business relations;
- upon carrying out a one-time operation (transaction) or several interconnected one-time operations (transactions) for the purchase and sale (exchange) of cash national and/or foreign currency in an amount equal to or exceeding 1,000,000 soms or the equivalent in foreign currency;
- upon carrying out a one-time electronic money transfer or carrying out an operation

- при совершении разового электронного денежного перевода или осуществлении операции (сделки) с виртуальными активами на сумму, равную или превышающую 100000 сомов или эквивалента в иностранной валюте;
- при наличии подозрения в осуществлении финансирования преступной деятельности и легализации (отмывания) преступных доходов, независимо от статуса клиента (постоянный или разовый) или любых исключений либо независимо от пороговой суммы операции (сделки);
- при выявлении фактов недостоверности или недостаточности ранее полученных сведений о клиенте.
- при совершении разовой операции (сделки) или нескольких взаимосвязанных разовых операций (сделок) по купле-продаже (обмену) наличной национальной и/или иностранной валюты на сумму от 100000 сомов до 1000000 сомов или эквивалента в иностранной валюте, проводится установление личности клиента на основе документа, удостоверяющего личность, проверка клиента на наличие или отсутствие в Санкционных перечнях и Перечне лиц, групп и организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов, и учет совершенной операции (сделки).

Между тем, независимо от суммы операции (сделки), статуса клиента и наличия формальных пороговых значений, Компания применяет меры внутреннего контроля, основанные на риск-ориентированном подходе, включая мониторинг операций (сделок) и анализ поведения клиента. При выявлении признаков повышенного риска, включая признаки дробления операций, несоответствия операций финансовому профилю клиента либо иных обстоятельств, свидетельствующих о возможной вовлеченности в ПФПД ЛПД, Компания осуществляет надлежащую проверку клиента и иные предусмотренные законодательством Кыргызской Республики меры.

6.3. Меры надлежащей проверки клиента:

6.3.1. Меры надлежащей проверки клиента применяются к новым и действующим клиентам, с учетом ранее проведенной надлежащей проверки клиента и уровня риска клиента.

6.3.2. К мерам надлежащей проверки относятся процедуры проведения идентификации, верификации клиента, его бенефициарного собственника.

(transaction) with virtual assets in an amount equal to or exceeding 100,000 soms or the equivalent in foreign currency;

- where there is suspicion of financing of criminal activity and legalization (laundering) of criminal proceeds, regardless of the status of the client (permanent or one-time) or any exceptions, or regardless of the threshold amount of the operation (transaction);

- upon identification of facts of unreliability or insufficiency of previously obtained information about the client;

- upon carrying out a one-time operation (transaction) or several interconnected one-time operations (transactions) for the purchase and sale (exchange) of cash national and/or foreign currency in an amount from 100,000 soms to 1,000,000 soms or the equivalent in foreign currency, the identity of the client is established on the basis of an identity document, the client is checked for the presence or absence in the Sanctions Lists and the List of persons, groups and organizations in respect of whom there is information on their participation in legalization (laundering) of criminal proceeds, and the carried out operation (transaction) is recorded.

Meanwhile, regardless of the transaction amount, the client's status, or the existence of formal thresholds, the Company implements internal control measures based on a risk-based approach, including transaction monitoring and analysis of client behavior. Upon identifying signs of increased risk, including signs of transaction fragmentation, transactions inconsistent with the client's financial profile, or other circumstances indicating possible involvement in money laundering or terrorist financing, the Company conducts an appropriate client verification and other measures provided for by the legislation of the Kyrgyz Republic.

6.3. Customer due diligence measures:

6.3.1. Customer due diligence measures are applied to new and existing clients, taking into account previously conducted customer due diligence and the client's risk level.

6.3.2. Due diligence measures include procedures for conducting identification and verification of the client and his beneficial owner.

6.3.3. Identification of the client is carried out by filling out the questionnaire of an individual client or the questionnaire of a legal entity client in the forms established by the legislation of the Kyrgyz Republic. Identification of a client establishing business relations and carrying out operations (transactions) remotely (distance method) is carried out in the manner established by the legislation of the Kyrgyz Republic.

6.3.3. Идентификация клиента производится путем заполнения анкеты клиента - физического лица или анкеты клиента - юридического лица по формам установленным законодательством Кыргызской Республики. Идентификация клиента, устанавливающего деловые отношения и осуществляющего операции (сделки) удаленным (дистанционным) способом, проводится в порядке, установленном законодательством Кыргызской Республики.

6.3.4. Специалист Компании, обслуживающий клиента, обязан провести идентификацию клиента Компании, до вступления Компании с клиентом (~~постоянного или разового клиента~~) в договорные отношения и предоставления ему услуг Оператора виртуальных активов. В случае если от имени или по поручению клиента выступает доверенное лицо, Компания обязана идентифицировать, это лицо, также путем заполнения соответствующей анкеты клиента. Идентификация клиента производится путем заполнения анкеты клиента - физического лица или анкеты клиента - юридического лица соответствующей формы.

6.3.5. В сроки, не превышающие пять рабочих дней с момента подачи заявки на открытие Учетной записи, сотрудник Компании должен провести верификацию информации, указанной:

а) в заявлении физического лица с использованием, по крайней мере, одного из следующих методов:

- подтверждение информации из официальных документов. В качестве документа для подтверждения могут быть использованы документы, удостоверяющие личность, перечисленные в пункте 5.7. настоящей Программы;

- осуществление контакта с клиентом по телефону, письмом или по электронной почте для подтверждения, предоставленной клиентом информации. При этом отключенный телефон, возвращенные письма или неработающие адреса электронной почты должны обуславливать продолжение проверки полученной информации;

- подтверждение легальности документов клиента, к примеру, через посольства, представительства Кыргызской Республики, нотариуса;

- иным методом, не противоречащим законодательству Кыргызской Республики.

б) в заявлении юридического лица, с использованием, по крайней мере, одного из следующих методов:

6.3.4. A Company specialist servicing the client is obliged to carry out identification of the Company's client before the Company enters into contractual relations with the client (~~a permanent or one-time client~~) and provides him with the services of the Virtual Asset Operator. In the event that an authorized representative acts on behalf of or by order of the client, the Company is obliged to identify this person as well by filling out the relevant client questionnaire. Identification of the client is carried out by filling out the questionnaire of an individual client or the questionnaire of a legal entity client of the relevant form.

6.3.5. Within a period not exceeding five working days from the moment of submission of an application for opening an Account, an employee of the Company must carry out verification of the information specified:

a) in the application of an individual, using at least one of the following methods:

- confirmation of information from official documents. As a document for confirmation, identity documents listed in paragraph 5.7. of this Program may be used;

- making contact with the client by telephone, letter or by electronic mail in order to confirm the information provided by the client. At the same time, a disconnected telephone, returned letters or non-working electronic mail addresses must entail continuation of verification of the received information;

- confirmation of the legality of the client's documents, for example, through embassies, representative offices of the Kyrgyz Republic, a notary;

- by another method not contradicting the legislation of the Kyrgyz Republic.

b) in the application of a legal entity, using at least one of the following methods:

- obtaining information from a state body for the purpose of checking the declared documents, whether the legal entity has been closed, liquidated or is in the process of liquidation;

- making contact with the client by telephone in order to confirm the information after opening the account;

- by another method not contradicting the legislation of the Kyrgyz Republic.

6.3.6. If in the process of verification of the client there arises doubt as to the reliability of the information obtained in the process of identification, and also if:

- a significant operation occurs (for example, in an amount exceeding the average balance or turnover on the client's account) and/or an operation not characteristic of the activity of this client;

- получение информации у государственного органа с целью проверки заявленных документов, не было ли юридическое лицо закрыто, ликвидировано или находится в процессе ликвидации;

- осуществление контакта с клиентом по телефону для подтверждения информации после открытия счета;

- иным методом, не противоречащим законодательству Кыргызской Республики.

6.3.6. Если в процессе верификации клиента возникает сомнение в достоверности информации, полученной в процессе идентификации, а также если:

- происходит значительная операция (например, на сумму, превышающую средний остаток или оборот по счету клиента) и/или операция, не характерная для деятельности данного клиента;

- наблюдаются значительные изменения в порядке ведения работы по счету клиента;

- Компания осознает, что ему недостаточно имеющейся информации о клиенте.

В этом случае Компании следует предпринять дополнительные запросы или сверку информации, которые могут включать следующее:

- персональные рекомендации (к примеру, от постоянного клиента Компании);

- рекомендации от Компании, ранее обслуживавшего данного клиента;

- справку с места работы, официальное подтверждение занимаемой должности (где применимо).

6.3.7. Компания принимает от Клиентов копии идентификационных документов и проверяет их путем сравнения с оригиналами или нотариально заверенными и легализованными копиями, или принимает такие копии для идентификации, чтобы избежать открытия счетов фиктивным лицам. Сотрудник Компании осуществляет идентификацию Клиента и бенефициарного владельца, таким образом, чтобы, в пределах своих возможностей, не допустить предоставление в Компанию недействительных или поддельных идентификационных документов. Также, для идентификации клиента, установления и идентификации бенефициарного владельца Компания проводит анкетирование.

6.3.8. Сотрудник Компании, принимающий идентификационный документ, должен проверить срок действия документа. Запрещается принимать документ с истекшим сроком действия.

- significant changes are observed in the procedure for conducting work on the client's account;

- the Company realizes that the information it has on the client is insufficient for it.

In this case, the Company should undertake additional inquiries or reconciliation of information, which may include the following:

- personal recommendations (for example, from a permanent client of the Company);

- recommendations from a Company that previously serviced this client;

- a certificate from the place of work, official confirmation of the position held (where applicable).

6.3.7. The Company accepts from Clients copies of identification documents and checks them by comparing them with originals or notarized and legalized copies, or accepts such copies for identification in order to avoid opening accounts for fictitious persons. An employee of the Company carries out identification of the Client and the beneficial owner in such a way as, within the limits of his capabilities, not to permit submission to the Company of invalid or forged identification documents. Also, for identification of the client, establishment and identification of the beneficial owner, the Company conducts a questionnaire survey.

6.3.8. An employee of the Company accepting an identification document must check the validity period of the document. It is prohibited to accept a document with an expired validity period.

6.3.9. If an employee of the Company has reasonable suspicions regarding the validity of documents, then the provided information must also be checked using open public registers and databases.

6.4. Identification of the client and his beneficial owner.

6.4.1. The Company is obliged to verify the identification data of the client, his authorized person (if any), and his beneficial owners.

6.4.2. The beneficial owner questionnaire is filled out in respect of the beneficial owner of new and existing clients.

6.4.3. The beneficial owner questionnaire is not filled out in respect of the following subjects:

- state authorities of the Kyrgyz Republic;

- local self-government bodies of the Kyrgyz Republic;

- widely known international organizations of which the Kyrgyz Republic is a member, the list of which is formed and published by the Ministry of Foreign Affairs of the Kyrgyz Republic.

6.4.4. In the absence of beneficial owners directly or indirectly (through third parties) owning more

6.3.9. Если у сотрудника Компании возникают обоснованные подозрения в действительности документов, то предоставленную информацию также необходимо проверить, используя открытые публичные регистры и базы данных.

6.4. Идентификация клиента и его бенефициарного владельца.

6.4.1. Компания обязана проверить идентификационные данные клиента, его уполномоченного лица (при наличии), его бенефициарных владельцев.

6.4.2. Анкета бенефициарного владельца заполняется в отношении бенефициарного владельца новых и действующих клиентов.

6.4.3. Анкета бенефициарного владельца не заполняется в отношении следующих субъектов:

- органы государственной власти Кыргызской Республики;
- органы местного самоуправления Кыргызской Республики;
- общеизвестные международные организации, членом которых является Кыргызская Республика, перечень которых формируется и публикуется Министерством иностранных дел Кыргызской Республики.

6.4.4. В случае отсутствия бенефициарных владельцев, прямо или косвенно (через третьих лиц) владеющих более 25% долей (акций) или имеются сомнения по размеру доли (акций) бенефициарного владельца либо не выявлен бенефициарный владелец в результате установления бенефициарного владельца клиента-юридического лица, то им может быть признано физическое лицо (физические лица), которое(ые) имеет(ют) возможность контролировать действия клиента-юридического лица за счет позиций, занимаемых в структуре юридического лица (ответственное за принятие стратегических решений, осуществляет исполнительный контроль, принимает решение по финансовым вопросам). В данном случае анкета бенефициарного владельца заполняется на данное лицо. При этом должны быть зафиксированы идентификационные данные известных бенефициарных владельцев.

6.4.5. В случае если бенефициарным владельцем клиента являются несколько физических лиц, каждый имеющий долю (акций) более 25%, то анкета заполняется на каждого бенефициарного владельца.

6.4.6. В случае если владельцем доли (акции) более 25% является юридическое лицо, необходимо выяснить и указать конкретное физическое лицо, которое, в конечном счете,

than 25% of shares (stocks), or where there are doubts as to the size of the share (stocks) of the beneficial owner, or the beneficial owner has not been identified as a result of establishing the beneficial owner of a client legal entity, such beneficial owner may be recognized as the individual (individuals) who has (have) the ability to control the actions of the client legal entity by virtue of positions occupied in the structure of the legal entity (responsible for making strategic decisions, carries out executive control, makes decisions on financial issues). In this case, the beneficial owner questionnaire is filled out for this person. At the same time, the identification data of known beneficial owners must be recorded.

6.4.5. In the event that the beneficial owners of the client are several individuals, each having a share (stocks) of more than 25%, the questionnaire is filled out for each beneficial owner.

6.4.6. In the event that the owner of a share (stock) of more than 25% is a legal entity, it is necessary to ascertain and indicate the specific individual who, ultimately, directly or indirectly (through third parties), owns (has predominant participation of more than 25% in the capital of) the legal entity or has the ability to control the actions of this legal entity. In this case, to the beneficial owner questionnaire it is necessary to attach a diagram of the ownership (management) structure of the client legal entity, which provides for intermediate legal entities up to the ultimate owners-individuals directly or indirectly (through third parties) owning more than 25% of shares (stocks), and the degree of interrelationship between the founder legal entities and the beneficial owner.

6.4.7. The Company re-identifies the Client and the beneficial owner if it has at its disposal information or suspicions arise about changes in the data certifying the identity of the Client or the Client's Representative, or the identification was carried out on the basis of invalid documents.

6.5. Verification of the beneficial owner.

6.5.1. The Company is obliged to apply reasonable measures for verification of the beneficial owner using documents, their copies compared with the original by an authorized person of the Company, or their copies certified by a notary, and (or) information obtained from reliable sources allowing the beneficial owner to be established.

6.5.2. The Company is obliged to verify the beneficial owner before or during the establishment of business relations with the client or the carrying out by the client of one-time operations (transactions), depending on the client's risk level.

6.5.3. When carrying out an operation (transaction) performed without the presence of the parties or

прямо или косвенно (через третьих лиц) владеет (имеет преобладающие участие более 25% в капитале) юридическим лицом либо имеет возможность контролировать действия этого юридического лица. В этом случае к анкете бенефициарного владельца необходимо приложить схему структуры собственности (управления) клиента-юридического лица, которая предусматривает промежуточные юридические лица, вплоть до конечных владельцев-физических лиц, прямо или косвенно (через третьих лиц) владеющих более 25% долей (акций), и степень взаимосвязи между учредителями-юридическими лицами и бенефициарным владельцем.

6.4.7. Компания, повторно идентифицирует Клиента и бенефициарного владельца, если в его распоряжении имеется информация или возникают подозрения об изменениях в данных, удостоверяющих личность Клиента или Представителя Клиента, или идентификация произведена на основании недействительных документов.

6.5. Верификация бенефициарного владельца.

6.5.1. Компания обязана применять разумные меры для верификации бенефициарного владельца с использованием документов, их копий, сверенных с оригиналом уполномоченным лицом Компании, или их копий, заверенных нотариусом, и (или) информации, полученной из достоверных источников, позволяющих установить бенефициарного владельца.

6.5.2. Компания обязана верифицировать бенефициарного владельца до или в ходе установления деловых отношений с клиентом или проведения клиентом разовых операций (сделок), в зависимости от уровня риска клиента.

6.5.3. При проведении операции (сделки), осуществляемой без присутствия сторон или с ценными бумагами, Компания завершает верификацию бенефициарного владельца в течение 10 календарных дней после установления деловых отношений с клиентом, если риски являются низкими. В данных случаях Компания должна до завершения верификации бенефициарного владельца применить процедуры управления рисками, включающие меры по ограничению количества, видов и (или) сумм операций (сделок), и мониторингу крупных и сложных операций (сделок).

6.5.4. Идентификация клиента юридического лица.

with securities, the Company completes verification of the beneficial owner within 10 calendar days after establishment of business relations with the client, if the risks are low. In these cases, before completion of verification of the beneficial owner, the Company must apply risk management procedures including measures to limit the number, types and (or) amounts of operations (transactions), and monitoring of large and complex operations (transactions).

6.5.4. Identification of the legal entity client. The client must provide the full package of required documents for opening an account and/or conducting by the Company an operation on paper medium or in the form of an electronic document.

6.5.5. When opening an Account and carrying out operations on the account of a client legal entity, the Company must verify the powers and authenticity of persons (on the basis of an identity document) having the right to dispose of monetary funds located in the client's account.

6.5.6. When studying documents, in particular constituent documents of a legal entity and documents confirming its state registration, for a more thorough study of its client, employees must pay special attention to legalization of documents, and also study:

- all constituent documents of the legal entity client, including all registered amendments and additions thereto, as well as other necessary documents confirming the state registration of the client as a legal entity;

- the composition of founders (participants) of the legal entity, determine persons having the possibility to influence the making of decisions by the bodies of the legal entity;

- the structure of the management bodies of the legal entity and their powers.

6.5.7. In the event that a third person opens an Account in the name of the client, the Company must obtain from the third person information and documents allowing identification and study of the client in whose name the account is opened and the third person opening the account.

6.5.8. For opening by a third person of an Account in the name of the client, a power of attorney executed in accordance with the requirements of the legislation of the Kyrgyz Republic for the right to open and (or) dispose of the Account must also be presented. Presentation of a power of attorney is not required from a representative of a legal entity authorized to open Accounts in accordance with the legislation of the Kyrgyz Republic, or the constituent documents of this legal entity.

6.5.9. When opening an Account, it is necessary to check for the presence/absence of the name (full name) of the client in the list of individuals and

Клиентом должен быть предоставлен полный пакет требуемых документов для открытия счета и/или проведения Компанией операции на бумажном носителе или в форме электронного документа.

6.5.5. При открытии Учетной записи и проведении операций по счету клиента - юридического лица Компания должна удостовериться в полномочиях и подлинности лиц (на основании документа, удостоверяющего личность), имеющих право распоряжаться денежными средствами, находящимися на счете клиента.

6.5.6. При изучении документов, в частности, учредительных документов юридического лица и документов, подтверждающих его государственную регистрацию, для более тщательного изучения своего клиента сотрудники должны обращать особое внимание на легализацию документов, а также изучить:

- все учредительные документы юридического лица - клиента, включая все зарегистрированные изменения и дополнения к ним, а также другие необходимые документы, подтверждающие государственную регистрацию клиента в качестве юридического лица;

- состав учредителей (участников) юридического лица, определить лиц, имеющих возможность влиять на принятие решений органами юридического лица;

- структуру органов управления юридического лица и их полномочия.

6.5.7. В случае, если третье лицо открывает Учетную запись на имя клиента, Компания должна получить от третьего лица информацию и документы, позволяющие идентифицировать и изучить клиента, на имя которого открывается счет и третье лицо, открывающее счет.

6.5.8. Для открытия третьим лицом Учетной записи на имя клиента также должна быть представлена доверенность, оформленная в соответствии с требованиями законодательства Кыргызской Республики, на право открытия и (или) распоряжения Учетной записью. Представление доверенности не требуется представителю юридического лица, уполномоченному открывать Учетные записи в соответствии с законодательством Кыргызской Республики, либо учредительными документами данного юридического лица.

6.5.9. При открытии Учетной записи, необходимо проверить на наличие/отсутствие имени (ФИО) клиента в перечне физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об их

legal entities, groups and organizations in respect of whom there is information on their participation in terrorist or extremist activity and proliferation of weapons of mass destruction, determined by the SFRS, as well as in other lists.

6.5.10. The Company has no right to open and maintain anonymous accounts, bearer accounts (deposits), and carry out any operations without identification of the correspondent Company, clients, and establishment of the beneficial owner in accordance with the requirements of the legislation of the Kyrgyz Republic.

6.5.11. For carrying out operations (transactions), the Company must provide in the Agreement for provision of services of the Virtual Asset Operator the obligations of the client to comply with the legislation on countering the financing of criminal activity and legalization (laundering) of criminal proceeds, as well as to provide supporting documents on conducted operations upon the Company's request.

6.6. The following documents are accepted for identification of individuals:

1. for citizens of the Kyrgyz Republic:
 - identification card — passport of a citizen of the Kyrgyz Republic (ID card);
 - general civil passport of a citizen of the Kyrgyz Republic;
 - ~~- birth certificate — for citizens of the Kyrgyz Republic under 16 years of age;~~
 - military card;
 - national driver's license containing the personal identification number (PIN);
2. in respect of foreign citizens:
 - passport of a foreign citizen;
 - residence permit in the Kyrgyz Republic;
 - ~~3. in respect of stateless persons — residence permit in the Kyrgyz Republic;~~
 - ~~4. in respect of refugees: — certificate of registration of an application for recognition of a person as a refugee; — refugee certificate.~~

6.7. Verification of the client. For verification of a client legal entity, the Company uses the following documents:

- decision of the founder(s) on creation of the legal entity;
- charter and foundation agreement;
- certificate of state registration (re-registration) of the legal entity;
- amendments to constituent documents — upon re-registration of the legal entity (if any);
- document confirming registration with the tax authority;
- documents confirming the powers of persons having the right of first and second

участии в террористической или экстремистской деятельности и распространения оружия массового уничтожения, определенном ГСФР, а также в иных списках.

6.5.10. Компания не имеет права открывать и вести анонимные счета, счета (вклады) на предъявителя и осуществлять любые операции без идентификации Компании-корреспондента, клиентов и установления бенефициарного владельца в соответствии с требованиями законодательства Кыргызской Республики.

6.5.11. Для проведения операций (сделок) Компания должна предусмотреть в Договоре на предоставление услуг Оператора виртуальных активов, обязательства клиента по соблюдению законодательства по противодействию финансированию преступной деятельности и легализации (отмыванию) преступных доходов, а также по предоставлению подтверждающих документов по проведенным операциям по запросу Компании.

6.6. Для удостоверения личности физических лиц принимаются следующие документы:

1) для граждан Кыргызской Республики:

- идентификационная карта - паспорт гражданина Кыргызской Республики (ID-карта);

- общегражданский паспорт гражданина Кыргызской Республики;

~~- свидетельство о рождении для граждан Кыргызской Республики, не достигших 16 летнего возраста;~~

- военный билет;

- водительское удостоверение национального образца, содержащее персональный идентификационный номер (ПИН);

2) в отношении иностранных граждан:

- паспорт иностранного гражданина;

- вид на жительство в Кыргызской Республике;

~~3) в отношении лиц без гражданства — вид на жительство в Кыргызской Республике;~~

~~4) в отношении беженцев:~~

~~свидетельство о регистрации ходатайства о признании лица беженцем;~~

~~удостоверение беженца.~~

6.7. Верификация клиента.

Для верификации клиента- юридического лица, Компания использует следующие документы:

- решение учредителя (лей) о создании юридического лица;

- устав и учредительный договор;

signature in the card with specimen signatures and seal impression;

- licenses for the right to carry out entrepreneurial activity (if any);

- and may also use other documents requested at the discretion of the Company itself.

6.7.1. The Company is obliged to verify the client by checking the reliability of the information provided in the questionnaire of the individual client or the questionnaire of the legal entity client, using information and documents obtained from reliable sources, within periods not exceeding ten working days after submission of the application for opening an Account.

6.7.2. The Company is obliged to verify the client before or during the establishment of business relations with the client or the carrying out by the client of one-time operations (transactions). Verification of the client during the establishment of business relations with the client when opening an account must be completed before the first financial operation on it is carried out.

6.7.3. When carrying out an operation (transaction) performed without the presence of the parties, the Company completes verification of the client within 10 calendar days after establishment of business relations, if the risks are low. In these cases, before completion of verification of the client, the Company must apply internal risk management procedures including measures to limit the number, types and (or) amounts of operations (transactions), as well as monitoring of large and complex operations (transactions).

6.7.4. When verifying the client, the Company must use original documents valid on the date of their presentation, obtained, including with the help of technical means, or copies compared with the original by an authorized person of the Company, or copies certified by a notary. If only part of a document relates to verification of the client, an extract from it certified by a notary may be presented. The client shall provide a translation of the document into the state or official language certified by a translation institution or by notarization. In the event of presentation of copies of documents, the Company must require presentation of original documents for familiarization and comparison; presentation of original documents by a method of remote identification and verification not contradicting the legislation of the Kyrgyz Republic shall be equated to presentation of original documents.

6.7.5. In the event that documents are drawn up wholly or partly in a foreign language, the Company must request from the client a translation of the document into the state or official language certified by a translation institution or by

- свидетельство о государственной регистрации (пререгистрации) юридического лица;
 - изменения в учредительные документы - при пререгистрации юридического лица (при наличии);
 - документ, подтверждающий постановку на учет в налоговом органе;
 - документы, подтверждающие полномочия лиц, имеющих право первой и второй подписи в карточке с образцами подписей и оттиском печати;
 - лицензии на право осуществления предпринимательской деятельности (при наличии).
- а также может использовать иные документы, запрошенные по усмотрению самой Компании.

6.7.1. Компания обязана верифицировать клиента путем проверки достоверности сведений, предусмотренных в анкете клиента - физического или анкете клиента - юридического лица, с использованием информации и документов, полученных из достоверных источников, в сроки, не превышающие десять рабочих дней после подачи заявки на открытие Учетной записи.

6.7.2. Компания обязана верифицировать клиента до или в ходе установления деловых отношений с клиентом или проведения клиентом разовых операций (сделок). Верификация клиента в ходе установления деловых отношений с клиентом при открытии счета должна быть завершена до осуществления по нему первой финансовой операции.

6.7.3. При проведении операции (сделки), осуществляемой без присутствия сторон, Компания завершает верификацию клиента в течение 10 календарных дней после установления деловых отношений, если риски являются низкими. В данных случаях Компания должна до завершения верификации клиента применить внутренние процедуры управления рисками, включающие меры по ограничению количества, видов и (или) сумм операций (сделок), а также мониторингу крупных и сложных операций (сделок).

6.7.4. При верификации клиента Компания должна использовать подлинники документов, действительные на дату их предъявления полученные в том числе с помощью технических средств, или в копиях, сверенных с оригиналом уполномоченным лицом Компании, или копиях, заверенных нотариально. Если к верификации клиента имеет отношение только часть документа,

notarization. Documents originating from state bodies of foreign states confirming the status of non-resident legal entities are accepted by the Company in the event of their legalization (apostille) in accordance with the Instruction on the procedure and conditions for affixing an apostille approved by Resolution of the Government of the Kyrgyz Republic dated November 18, 2010 No. 283. These documents may be presented without their legalization (apostille) in cases provided for by international treaties that have entered into force in the manner established by law and to which the Kyrgyz Republic is a party.

6.7.6. When verifying the client, the Company may also use additional (auxiliary) information obtained from reliable sources. The Company applies to authorized state bodies to obtain information on the status of the client legal entity (active, liquidated or in the process of liquidation).

6.7.7. In the event that an authorized representative acts on behalf of the client, the Company is obliged to verify him and also check the relevant documents confirming the powers of such person. In addition to identification of the client, essential importance is attached to study of the client's economic or professional activity, as well as his income and sources of assets. The Company studies the economic activity of its clients, being guided by the following principles and carrying out the following actions and measures:

- obtains information from the Client before the beginning of cooperation, so as to:
- know the main directions of the Clients' economic activity;
- identify transactions typical for the client according to the received information.
- when carrying out operations on the Client's account, it is necessary to request documents on the basis of which the operation subject to checking for compliance with the signs of a suspicious transaction and operation is carried out;
- the Company exercises supervision over operations carried out on the Client's accounts, forms and updates data on the Client's economic activity, and considers the question of further cooperation with the Client if such cooperation may damage the reputation of the Company.

Copies of identification documents of the Client and the beneficial owner and the information necessary for identification must be stored in the Company in the Client's file for not less than 5 years. The said period shall be calculated from the day of termination of relations with the client.

6.8. Work with clients for the purposes of CFCA/LCP, purpose of payment when replenishing the Account.

может быть представлена выписка из него, заверенная нотариусом. Клиент предоставляет перевод документа на государственный или официальный язык, заверенный переводческим учреждением или нотариально. В случае представления копии документов, Компания должна потребовать представления подлинников документов для ознакомления и сверки, представление подлинников документов, методом удаленной идентификации и верификации, не противоречащим законодательству Кыргызской Республики, приравнивается к представлению подлинников документов.

6.7.5. В случае если документы составлены полностью или частично на иностранном языке, Компания должна затребовать от клиента перевод документа на государственный или официальный язык, заверенный переводческим учреждением или нотариально. Документы, исходящие от государственных органов иностранных государств, подтверждающие статус юридических лиц-нерезидентов, принимаются Компанией в случае их легализации (апостиль) в соответствии с Инструкцией о порядке и условиях проставления апостиля, утвержденной постановлением Правительства Кыргызской Республики от 18 ноября 2010 года No 283. Указанные документы могут быть представлены без их легализации (апостиля) в случаях, предусмотренных международными договорами, вступившими в установленном законом порядке в силу, участницей которых является Кыргызская Республика.

6.7.6. Компания при верификации клиента также может использовать дополнительную (вспомогательную) информацию, полученную из достоверных источников. Компания обращается в уполномоченные государственные органы для получения информации о статусе клиента - юридического лица (действует, ликвидирован или находится в процессе ликвидации).

6.7.7. В случае если от имени клиента выступает доверенное лицо, Компания обязана его верифицировать, а также проверить соответствующие документы, подтверждающие полномочия такого лица. Кроме идентификации клиента существенное значение имеет изучение хозяйственной или профессиональной деятельности клиента, а также его доходов и источников активов. Компания изучает хозяйственную деятельность своих клиентов, руководствуясь следующими принципами и осуществляя следующие действия и мероприятия:

6.8.1. The Company tracks transactions (operations) on the client's Account for the purposes of CFCA/LCP.

6.8.2. When replenishing the Account, the client must indicate in the purpose of payment his Unique Client Identification Number for the purpose of delimitation and identification of funds received from the client. In the event that the Company has doubt regarding the legality of the client's monetary funds, the Company has the right to require the client to provide documents confirming the legality of the monetary funds. Such documents may be invoices issued to the client, contracts concluded by the client, payment documents (for example, invoices, bills of lading), declarations, etc.

6.8.3. In the event of refusal by the client to provide the required documents, the Company has the right to refuse to carry out an operation on the account. This condition must be stipulated in the Account agreement between the Company and the client.

6.8.4. The Company employee servicing the client tracks operations on clients' accounts. The Company must have an understanding of normal and reasonable activity on the accounts of its clients in order to identify operations not characteristic of this client.

6.8.5. A Company employee servicing the client should pay attention to operations (transactions) of the client irrational from an economic or commercial point of view, operations with large sums of cash monetary funds (for example, exceeding the average turnovers for transactions and operations of this client), and other operations not corresponding to the usual practice of the client.

6.8.6. For the purpose of recognizing unusual or suspicious accounts, the Company establishes key indicators of such accounts, taking into account general information about the client, for example, information about the country of origin and the source of funds, the type of operation and other risk factors.

6.8.7. In respect of unusual or suspicious operations, the Company must determine whether the client is acting on behalf of another person and then take steps to obtain data for establishing the identity of this other person, the beneficial owner.

6.8.8. When determining the beneficial owner in respect of legal entities, special attention must be paid to shareholders, persons with the right of signature or other persons who have a significant share in the capital, or who in any other manner exercise control over the client. In the event that the owner is another legal entity, the Company must establish the owners or persons exercising control over this legal entity.

- получает информацию от Клиента до начала сотрудничества, с тем чтобы:

- знать основные направления хозяйственной деятельности Клиентов;
- идентифицировать типичные для клиента сделки, согласно полученной информации.

- при проведении операций по счету Клиента, необходимо затребовать документы, на основании которых осуществляется операция, подлежащая проверке на предмет соответствия признакам подозрительной сделки и операции;

- Компания осуществляет надзор над операциями, осуществляемыми по счетам Клиента, формирует и обновляет данные о хозяйственной деятельности Клиента, рассматривает вопрос о дальнейшем сотрудничестве с Клиентом, если такое сотрудничество может повредить репутации Компании.

Копии идентификационных документов Клиента и бенефициарного владельца и сведения, необходимые для идентификации, должны храниться в Компании в деле Клиента не менее 5 лет. Указанный срок исчисляется со дня прекращения отношений с клиентом.

6.8. Работа с клиентами в целях ПФПД ЛПД, назначение платежа при пополнении Счета.

6.8.1. Компания отслеживает сделки (операции) по Учетной записи клиента в целях ПФПД ЛПД.

6.8.2. При пополнении Учетной записи клиент должен указать в назначении платежа свой Уникальный идентификационный номер клиента с целью разграничения и идентификации полученных от клиента средств. В случае, если у Компании появляется сомнение в законности денежных средств клиента, Компания имеет право требовать у клиента предоставить документы, подтверждающие законность денежных средств. Такими документами могут быть счета, выставленные клиенту, договора, заключенные клиентом, платежные документы (к примеру, инвойсы, счета-фактуры), декларации и т.д.

6.8.3. В случае отказа клиента предоставить требуемые документы Компания имеет право отказать в проведении операции по счету. Данное условие должно быть оговорено в договоре Учетной записи между Компанией и клиентом.

6.8.4. Сотрудник Компании, обслуживающий клиента, отслеживает операции по счетам

6.8.9. If necessary, the Company may use sources of information available to it on lawful grounds.

6.8.10. The conclusions made by the Company in respect of suspicious operations must be documented and stored for not less than five years from the moment the operation is carried out.

клиентов. Компания должна иметь понятие о нормальной и разумной деятельности по счетам своих клиентов для того, чтобы выявлять операции, нехарактерные для данного клиента.

6.8.5. Сотруднику Компании обслуживающего клиента следует обращать внимание на нерациональные с экономической или коммерческой точки зрения операции (сделки) клиента, операции с большими суммами наличных денежных средств (например, превышающие средние обороты по сделкам и операциям данного клиента) и другие операции, не соответствующие обычной практике клиента.

6.8.6. В целях распознавания необычных или подозрительных счетов Компания устанавливает ключевые показатели таких счетов, учитывая общую информацию о клиенте, например, сведения о стране происхождения и об источнике средств, тип операции и прочие факторы риска.

6.8.7. В отношении необычных или подозрительных операций Компания должна определить действует ли клиент от имени другого лица и затем предпринять шаги для получения данных для установления личности этого другого лица бенефициарного владельца.

6.8.8. При определении бенефициарного владельца в отношении юридических лиц особое внимание должно уделяться акционерам, лицам с правом подписи или другим лицам, которые имеют значительную долю в капитале, или каким-либо другим способом осуществляют контроль над клиентом. В случае, если владельцем является другое юридическое лицо, Компании необходимо установить владельцев или лиц, осуществляющих контроль над данным юридическим лицом.

6.8.9. В случае необходимости Компанией могут использоваться источники информации, доступные ему на законных основаниях.

6.8.10. Выводы, сделанные Компанией в отношении подозрительных операций, должны быть задокументированы и храниться не менее пяти лет с момента осуществления операции.

7. ПРОЦЕДУРА ОПРЕДЕЛЕНИЯ УРОВНЯ РИСКА КЛИЕНТА

7.1. Процесс идентификации и изучения клиентов и бенефициарных владельцев включает также, определение уровня риска по осуществлению клиентом финансирования преступной деятельности и легализации преступных доходов, установленных законодательством Кыргызской Республики.

7. PROCEDURE FOR DETERMINING THE CLIENT'S RISK LEVEL

7.1. The process of identification and study of clients and beneficial owners also includes determination of the risk level of the client's carrying out financing of criminal activity and legalization of criminal proceeds established by the legislation of the Kyrgyz Republic. In connection with this, the Company is obliged to:

В связи с чем, Компания обязана:

- оценивать, определять, документально фиксировать и постоянно обновлять риски с учетом результатов национальной оценки рисков и типичных критериев высоких и низких рисков и настоящей Программой;
- в установленном порядке представлять информацию о выявленных рисках руководителю Компании и органу финансовой разведки КР;
- разрабатывать и применять усиленную, стандартную или упрощенную проверку, а также меры контроля, процедуры по управлению и снижению рисков.

7.1.1. Компания на основании Положения о надлежащей проверке клиента, утвержденной постановлением Кабинета министров Кыргызской Республики от 14 ноября 2025 года № 739, глава 3 пункт 11, при проведении надлежащей проверки клиента применяет усиленные меры - «высокий риск», стандартные меры - «средний риск», упрощенные меры - «низкий риск» надлежащей проверки клиента с использованием риск-ориентированного подхода.

7.1.2. Компания обязана классифицировать своих клиентов с учетом критериев риска (высокий, средний и низкий). Для определения уровня риска необходимо как минимум принимать во внимание вид деятельности Компании, клиента и местонахождение (происхождение) клиента и/или его бизнеса, а также проводимые им операции, оказываемые услуги. Бизнес-профиль компании, деятельность которой связана с операциями с виртуальными активами, предполагает предоставление услуг местным и международным клиентам на международных рынках. Особенности бизнеса Компании, изложенные выше, определяют значительную географическую дистанцию между самой Компанией и ее клиентами. В связи с чем, клиенты-нерезиденты для Компании относятся к среднему уровню риска, к которым применяются стандартные меры надлежащей проверки, при отсутствии у таких клиентов признаков высокого риска.

7.1.3. На основании всей информации и документов, позволяющих идентифицировать, верифицировать и изучить клиента, Компанией оценивается уровень риска осуществления клиентом возможного финансирования преступной деятельности и легализации (отмывания) преступных доходов, который отражается в анкете клиента.

7.1.4. Компания должна уделять особое внимание и осуществлять надлежащий

- assess, determine, document and constantly update risks taking into account the results of the national risk assessment and typical criteria of high and low risks and this Program;

-in the established manner submit information on identified risks to the head of the Company and the financial intelligence authority of the Kyrgyz Republic;

- develop and apply enhanced, standard or simplified due diligence, as well as control measures, risk management and mitigation procedures.

7.1.1. Based on the Regulation on customer due diligence approved by Resolution of the Cabinet of Ministers of the Kyrgyz Republic dated November 14, 2025 No. 739, Chapter 3, paragraph 11, when conducting customer due diligence, the Company applies enhanced measures – “high risk,” standard measures – “medium risk,” simplified measures – “low risk” of customer due diligence using a risk-based approach.

7.1.2. The Company is obliged to classify its clients taking into account risk criteria (high, medium and low). To determine the risk level, it is necessary at a minimum to take into account the type of activity of the Company, the client and the location (origin) of the client and/or his business, as well as the operations carried out by him and the services rendered. The business profile of a company whose activities are related to transactions with virtual assets involves the provision of services to local and international clients in international markets. The peculiarities of the Company’s business set out above determine a significant geographical distance between the Company itself and its clients. In this regard, non-resident clients for the Company are classified as medium risk, to whom standard customer due diligence measures apply, in the absence of signs of high risk in such clients.

7.1.3. On the basis of all information and documents allowing identification, verification and study of the client, the Company assesses the level of risk of the client’s possible financing of criminal activity and legalization (laundering) of criminal proceeds, which is reflected in the client questionnaire.

7.1.4. The Company should pay special attention and exercise proper control in respect of the Company’s operations exposed to high risk of financing of criminal activity and legalization (laundering) of criminal proceeds, and conducting operations having signs of suspicious operations.

7.1.5. If a high risk level is established, the Company applies the following enhanced customer due diligence measures:

- collection of additional identification information and documents in respect of the client from

контроль в отношении операций Компании, подверженных высокому риску осуществления финансирования преступной деятельности и легализации (отмывания) преступных доходов, и проведения операций, имеющих признаки подозрительных операций.

7.1.5. В случае установления высокого уровня риска Компания применяет следующие усиленные меры надлежащей проверки клиента:

- сбор дополнительных идентификационных сведений и документов в отношении клиента из доступных и надежных источников информации, а также использование данных сведений при оценке риска, связанного с клиентом;
- сбор дополнительной информации о клиенте и бенефициарном владельце для глубокого понимания риска возможной вовлеченности такого клиента и бенефициарного владельца в преступную деятельность;
- запрос дополнительной информации у клиента относительно цели и предполагаемого характера деловых отношений, а также источника денежных средств клиента;
- проверка источников денежных средств клиента, используемых в рамках установления деловых отношений, для того чтобы убедиться, что денежные средства не являются доходами от преступной деятельности;
- регулярное обновление идентификационных данных клиента и бенефициарного владельца, но не реже одного раза в год;
- запрос у клиента дополнительной информации, разъясняющей причину или экономический смысл запланированных или проведенных операций (сделок);
- получение разрешения Директора на установление или продолжение деловых отношений с клиентом;
- осуществление усиленного мониторинга деловых отношений путем ежедневного мониторинга операций (сделок), анализа информации, рассмотрения и учета назначения денежных средств, с использованием как информационных автоматизированных систем, так и в ручном режиме, в целях выявления признаков подозрительных операций (сделок) и операций (сделок), не имеющих очевидного экономического смысла или очевидной законной цели, а также доведение результатов мониторинга до сведения должностного лица по ПФПД ЛПД и Директора;

available and reliable information sources, as well as use of this information when assessing risk associated with the client;

- collection of additional information about the client and beneficial owner for a deeper understanding of the risk of possible involvement of such client and beneficial owner in criminal activity;

- request for additional information from the client regarding the purpose and intended nature of business relations, as well as the source of the client's funds;

- verification of the sources of the client's funds used within the framework of establishing business relations in order to make sure that the funds are not proceeds of criminal activity;

- regular updating of identification data of the client and beneficial owner, but not less than once a year;

- request from the client for additional information explaining the reason or economic meaning of planned or conducted operations (transactions);

- obtaining the Director's permission to establish or continue business relations with the client;

- carrying out enhanced monitoring of business relations by daily monitoring of operations (transactions), analysis of information, review and accounting of the purpose of funds, using both information automated systems and manual mode, for the purpose of identifying signs of suspicious operations (transactions) and operations (transactions) having no obvious economic meaning or obvious lawful purpose, as well as bringing the results of monitoring to the attention of the official for CFCA/LCP and the Director.

7.1.6. Enhanced customer due diligence measures should also be applied to clients from high-risk countries.

7.1.7. If a medium risk level is established, the Company applies the following standard customer due diligence measures:

- obtaining general information about the purpose and intended nature of business relations;

- verification of the client and beneficial owner before establishment of business relations;

- monitoring of client operations (transactions), including using an automated verification system;

- collection of additional identification information and documents in respect of the client from available and reliable information sources, as well as use of this information when assessing risk associated with the client;

- collection of additional information about the client and beneficial owner for understanding the risk of possible involvement of such client and beneficial owner in criminal activity;

7.1.6. Усиленные меры надлежащей проверки клиента также должны применяться к клиентам из высокорискованных стран.

7.1.7. В случае установления среднего уровня риска Компания применяет следующие стандартные меры надлежащей проверки клиента:

- получение общей информации о цели и предполагаемом характере деловых отношений;
- верификация клиента и бенефициарного владельца до установления деловых отношений;
- мониторинг операций (сделок) клиента в том числе с использованием автоматизированной системы проверки;
- сбор дополнительных идентификационных сведений и документов в отношении клиента из доступных и надежных источников информации, а также использование данных сведений при оценке риска, связанного с клиентом;
- сбор дополнительной информации о клиенте и бенефициарном владельце для понимания риска возможной вовлеченности такого клиента и бенефициарного владельца в преступную деятельность;
- проверка источников происхождения денежных средств клиента, используемых в рамках установления деловых отношений, для того чтобы убедиться, что денежные средства не являются доходами от преступной деятельности;
- обновление идентификационных данных клиента, раз в три года.

7.1.8. В случае установления низкого риска Компания применяет следующие упрощенные меры надлежащей проверки клиента:

- получение общей информации о цели и предполагаемом характере деловых отношений;
- верификация клиента и бенефициарного владельца после установления деловых отношений;
- сокращение частоты обновления идентификационных данных клиента и бенефициарного владельца;
- мониторинг операций (сделок) клиента в сокращенной форме, с использованием автоматизированной системы проверки операций (сделок).
- обновление идентификационных данных клиента, раз в три года.

7.1.9. При обслуживании иностранных публичных должностных лиц Компания должна применить следующие меры:

- verification of the sources of origin of the client's funds used within the framework of establishing business relations in order to make sure that the funds are not proceeds of criminal activity;

- updating of the client's identification data once every three years.

7.1.8. If a low risk is established, the Company applies the following simplified customer due diligence measures:

- obtaining general information about the purpose and intended nature of business relations;

- verification of the client and beneficial owner after establishment of business relations;

- reduction of the frequency of updating the identification data of the client and beneficial owner;

- monitoring of the client's operations (transactions) in a reduced form using an automated operation (transaction) verification system;

- updating of the client's identification data once every three years.

7.1.9. When servicing foreign public officials, the Company must apply the following measures:

- use tools to determine whether the client or beneficial owner is a public official;

- obtain written permission from the head of the Company to establish or continue (for existing clients) business relations with a public official. Permission of the head is not required when a public official carries out a one-time operation;

- establish the source of origin of funds or other property of the foreign public official;

- conduct continuous and in-depth monitoring of business relations, including operations (transactions) carried out by the foreign public official, in the manner established for high-risk clients;

- on a permanent basis update information on foreign public officials available to it.

The Company must apply the above measures in respect of family members and close persons (close relatives, business partners and official representatives) of a foreign public official.

7.1.10. The measures specified in paragraph 6.1.9 also apply in respect of national public officials and public officials of international organizations, as well as their families and close persons in the event of determining a high risk of business relations with such persons.

7.1.11. When identifying national public officials, the Company records the information obtained in electronic format according to the public official questionnaire form established by the financial intelligence authority and, within 3 (three) working days, sends to the financial intelligence authority the information recorded in the national public

- использовать инструменты для определения того, является ли клиент или бенефициарный владелец публичным должностным лицом;
 - получить письменное разрешение руководителя Компании для установления или продолжения (для существующих клиентов) деловых отношений с публичным должностным лицом. Разрешение руководителя не требуется при совершении публичным должностным лицом разовой операции;
 - установить источник происхождения денежных средств или иного имущества иностранного публичного должностного лица;
 - проводить постоянный и углубленный мониторинг деловых отношений, в том числе операций (сделок), осуществляемых иностранным публичным должностным лицом, в порядке, установленном для клиентов высокого риска;
 - на постоянной основе обновлять имеющуюся в распоряжении информацию об иностранных публичных должностных лицах. Компания должна применить вышеуказанные меры в отношении членов семьи и близких лиц (близкие родственники, деловые партнеры и официальные представители) иностранного публичного должностного лица.
- 7.1.10. Меры, указанные в пункте 6.1.9., применяются также в отношении национальных публичных должностных лиц и публичных должностных лиц международных организаций, а также их семей и близких лиц в случае определения высокого риска деловых отношений с такими лицами.
- 7.1.11. При выявлении национальных публичных должностных лиц Компания фиксирует полученные сведения в электронном формате, согласно форме анкеты публичного должностного лица, установленной органом финансовой разведки, и в течение 3 (трех) рабочих дней направляют в орган финансовой разведки информацию, зафиксированную в анкете национального публичного должностного лица, по электронным каналам связи.
- 7.1.12. Компания может использовать открытые источники информации для установления, мониторинга и проверки информации в отношении публичных должностных лиц.
- 7.1.13. Компания должна обновлять сведения, полученные в результате идентификации, верификации и изучения клиента, а также установления бенефициарного владельца, периодически, не реже одного раза в год в

official questionnaire via electronic communication channels.

7.1.12. The Company may use open information sources to establish, monitor and verify information in respect of public officials.

7.1.13. The Company must update information obtained as a result of identification, verification and study of the client, as well as establishment of the beneficial owner, periodically, at least once a year in cases where the Company assesses the risk of the client's carrying out financing of criminal activity and legalization (laundering) of criminal proceeds as high, and in other cases at least once every three years.

7.1.14. The Company must ensure compliance with all procedures developed for the purpose of exercising proper control over the risk of financing of criminal activity and legalization (laundering) of criminal proceeds associated with the use of new technologies (new products) involving carrying out operations (transactions) without direct contact with the client.

7.1.15. When establishing correspondent relations, the Company must establish, including by sending a request to the correspondent Company, whether it carries out CFCA/LCP measures, including identification, verification and study by the correspondent Company of its clients.

7.2. Determination of the risk level

7.2.1. To determine the risk level, it is necessary, at a minimum, to take into account the type of activity of the client and the location (origin) of the client and/or his business.

7.2.2. The client and/or his beneficial owner is considered exposed to high risk of legalization (laundering) of proceeds obtained by criminal means and financing of terrorism if he meets at least one of the following criteria:

By type of client activity:

- activities of legal entities (their separate subdivisions) that are not credit organizations engaged in money transfers, cash payments, by checks, collection of funds;
- activities of legal entities (including credit organizations) registered in offshore zones, their separate subdivisions, subsidiaries and dependent companies;
- gambling business (entrepreneurial activity not involving sale of products (goods, works, services), associated with receipt by a gambling establishment (casino, totalizator, bookmaker's office, gaming machine hall and other gambling houses (places)) of income from participation in gambling in the form of winnings and payment for its conduct);
- activity connected with the sale, including commission sale, of objects of art and antiques;

случаях, когда Компания оценивает риск осуществления клиентом финансирования преступной деятельности и легализации (отмывания) преступных доходов, как высокий, и в иных случаях не реже одного раза в три года.

7.1.14. Компания должна обеспечить соблюдение всех процедур, разработанных в целях осуществления надлежащего контроля риска финансирования преступной деятельности и легализации (отмывания) преступных доходов, связанного с применением новых технологий (новых продуктов), предполагающих осуществление операций (сделок) без непосредственного контакта с клиентом.

7.1.15. При установлении корреспондентских отношений Компания должна установить, в том числе путем направления запроса Компании-корреспонденту, осуществляются ли им меры по ПФПД ЛПД, включая идентификацию, верификацию и изучение Компанией-корреспондентом его клиентов.

7.2. Определение уровня риска

7.2.1. Для определения уровня риска необходимо, как минимум, принимать во внимание вид деятельности клиента и место нахождения (происхождение) клиента и/или его бизнеса.

7.2.2. Клиент и (или) его бенефициарный владелец считается подверженным высокому риску осуществления легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма, если он отвечает хотя бы одному из следующих критериев:

По виду деятельности клиента:

- деятельность юридических лиц (их обособленных подразделений), не являющихся кредитными организациями, занимающихся переводом денежных средств, платежами в наличной форме, по чекам, инкассацией денежных средств;

- деятельность юридических лиц (в том числе кредитных организаций), зарегистрированных в оффшорных зонах, их обособленных подразделений, дочерних и зависимых обществ;

- игровой бизнес (предпринимательская деятельность, не являющаяся реализацией продукции (товаров, работ, услуг), связанная с извлечением игорным заведением (казино, тотализатор, букмекерская контора, зал игровых автоматов и иные игорные дома (места)) дохода от участия в азартных играх в виде выигрыша и платы за их проведение);

- trade (especially export) of precious metals, precious stones, as well as jewelry containing precious metals and precious stones;

- activities of legal entities carrying out operations mainly in cash form (large shopping complexes, restaurants, gas stations, etc.);

- activities of legal entities (their separate subdivisions) carrying out transactions with virtual assets as their main type of activity without obtaining the appropriate permits (licenses) for this type of activity.

By geographical factor:

- the client and/or his beneficial owner is registered or carries out his activity in an offshore zone;

- the client and/or his beneficial owner is registered or carries out his activity in high-risk countries according to the list of the SFRS KR;

The Company applies enhanced customer due diligence measures when establishing business relations and/or carrying out operations (transactions) with individuals or legal entities from high-risk countries.

By type of client:

- the Client is a non-commercial or charitable/trust organization;

- the Client, its directors, shareholders and/or true beneficiaries fall under the sanctions list provided for by the legislation of the Kyrgyz Republic, the Consolidated Sanctions List of the UN Security Council;

- the Client appears in such lists as Panama Papers, Mossack Fonseca, Paradise Papers;

- the Client, the true beneficiary of the client is a PDL, including foreign PDLs, members of their families or persons closely connected with them, or legal entities and legal funds whose true beneficiaries are the said persons;

- absence of information on the client (legal entity) in publicly available unified state registers of legal entities and on the Internet;

- the client legal entity was established less than 1 year ago;

- the ownership structure of the client legal entity consists of 3 or more levels;

- the Director of the client legal entity is "mass";

- the client legal entity has nominee shareholders or bearer shares;

- the client insufficiently provides information on the beneficial owner and/or refuses to disclose the beneficial owner;

- the client provides documents/information in respect of which there are doubts as to their reliability/authenticity;

- unclear source of origin of funds.

Adverse media:

- the Client, its directors or shareholders of the client were involved in CFCA/LCP scandals and/or

- деятельность, связанная с реализацией, в том числе комиссионной, предметов искусства и антиквариата;

- торговля (особенно экспорт) драгоценными металлами, драгоценными камнями, а также ювелирными изделиями, содержащими драгоценные металлы и драгоценные камни;

- деятельность юридических лиц, осуществляющих операции преимущественно в наличной форме (крупные торговые комплексы, рестораны, автозаправочные станции и т.п.);

- деятельность юридических лиц (их обособленных подразделений), осуществляющих сделки с виртуальными активами в качестве своего основного вида деятельности без получения на данный вид деятельности соответствующих разрешений (лицензий).

По географическому фактору:

- клиент и (или) его бенефициарный владелец зарегистрирован или осуществляет свою деятельность в оффшорной зоне;

- клиент и (или) его бенефициарный владелец зарегистрирован или осуществляет свою деятельность в высокорискованных странах, согласно перечню ГСФР КР;

Компания применяет усиленные меры надлежащей проверки клиента при установлении деловых отношений и (или) осуществлении операций (сделок) с физическими или юридическими лицами из высокорискованных стран.

По типу клиента:

- Клиент является некоммерческой или благотворительной/трастовой организацией;

- Клиент, его директора, акционеры и/или истинные бенефициары попадают под санкционный перечень, предусмотренный законодательством Кыргызской Республики, Сводным санкционным перечнем Совета Безопасности ООН;

- Клиент фигурирует в таких списках, как Panama Papers, Mossack Fonseca, Paradise Papers;

- Клиент, истинный бенефициар клиента является ПДЛ, в том числе иностранные ПДЛ, члены их семей или лица, тесно связанные с ними, или юридические лица и юридические фонды, истинными бенефициарами которых являются указанные лица;

- Отсутствие информации о клиенте (юридическом лице) в общедоступных единых государственных реестрах юридических лиц и в сети «Интернет»;

there is negative advertising / press articles within the framework of CFCA/LCP.

In the remaining part, one should be guided by the approved List of suspicious operations.

7.2.3. Assignment of a high risk level to the client entails application by the Company of enhanced customer due diligence measures for effective management and/or mitigation of risks.

7.2.4. The client and/or his beneficial owner is considered exposed to medium risk of legalization (laundering) of proceeds obtained by criminal means and financing of terrorism if he meets at least one of the following criteria, but there are no high-risk criteria:

By type of client:

- the client legal entity was established less than 2 years ago;

- frequent change of directors and/or legal address of the legal entity (more than 2 times within a year);

- the Client is a non-resident of the Kyrgyz Republic.

Adverse media:

- minor negative media attitude towards the Client, its directors or shareholders.

7.2.5. Assignment of a medium risk level to the Client entails application by the Company of standard customer due diligence measures for effective management and/or mitigation of risks.

7.2.6. In the absence of signs (criteria) of high or medium risk listed in clauses 5.2.2 and 5.2.4, the Client is assigned a low Risk level.

7.2.7. The Risk level is reviewed (updated) as factors affecting the risk assessment change or new signs (criteria) of Risk are identified (on the basis of events), and upon occurrence of review periods, but not less than once a year.

7.2.8. Review of the Client's Risk level is carried out in the following cases:

- in accordance with the period for updating information on the Client, but not less than once every 3 years;

- regardless of the period for updating information, from low or medium to high in the following cases:

- presence in the client's activity of operations subject to mandatory control, suspicious operations, information on which has been submitted to the authorized body;

- if the Company has received a request from the authorized body to provide information and/or documents on the Client and/or the Client's operations;

- in case of taking a decision in respect of the Client to refuse to execute his order to carry out an operation / transaction;

- regardless of the period for updating information, from low to medium level, or to high level, or from medium risk level to high level, if in the process of

- Клиент-юридическое лицо был основан менее 1 года назад;
- Структура собственности клиента-юридического лица состоит из 3 и более уровней;
- Директор Клиента-юридического лица является «массовым»;
- Клиент-юридическое лицо имеет номинальных акционеров или акции на предъявителя;
- Клиент в недостаточной степени представляет сведения о бенефициарном владельце и/или отказывается раскрывать бенефициарного владельца;
- Клиент предоставляет документы/сведения, в отношении которых имеются сомнения в их достоверности/подлинности;
- Неясный источник происхождения денежных средств;

Нежелательные СМИ:

- Клиент, его директора или акционеры клиента были замешаны в скандалах с ПФПД ЛПД и/или есть негативная реклама / статьи в прессе в рамках ПФПД ЛПД

В остальной части следует руководствоваться утверждённым Перечнем подозрительных операций.

7.2.3. Присвоение высокого уровня риска клиенту влечет применение Компанией усиленных мер надлежащей проверки клиента для эффективного управления и (или) снижения рисков.

7.2.4. Клиент и (или) его бенефициарный владелец считается подверженным среднему уровню риска осуществления легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма, если он отвечает хотя бы одному из следующих критериев, но при этом отсутствуют критерии высокого риска:

По типу клиента:

- Клиент-юридическое лицо был основан менее 2-х лет назад;
- Частая смена директоров и/или юридического адреса у юридического лица (более 2-х раз в течение года);
- Клиент является нерезидентом Кыргызской Республики;

Нежелательные СМИ:

- Незначительное негативное отношение СМИ к Клиенту, его директорам или акционерам.

7.2.5. Присвоение среднего уровня риска Клиенту влечет применение Компанией стандартных мер надлежащей проверки

internal control there arose grounds sufficient for revising the Client's Risk level;

- regardless of the period for updating information, from high to medium or low level, or from medium to low level, if in the process of internal control there arose grounds sufficient for revising the Client's Risk level.

7.2.9. In the event that the client's operations (transactions) are recognized as suspicious, on the day of recognition and sending of reports to the authorized body, the CO employee changes the "Risk degree" to "high." Changes in the risk level are recorded by the Company's authorized employee in the client's file.

клиента для эффективного управления и (или) снижения рисков.

7.2.6. В случае отсутствия признаков (критериев) высокого или среднего уровня риска, перечисленных в п. 5.2.2. и п. 5.2.4, Клиенту присваивается низкий уровень Риска.

7.2.7. Уровень Риска пересматривается (актуализируется) по мере изменения факторов, влияющих на оценку риска или выявления новых признаков (критериев) Риска (на основании событий) и при наступлении сроков пересмотра, но не реже одного раза в год.

7.2.8. Пересмотр уровня Риска Клиента осуществляется в следующих случаях:

- в соответствии со сроком обновления сведений о Клиенте, но не реже одного раза в 3 года;

- независимо от срока обновления сведений с низкого или среднего на высокий в следующих случаях:

- наличие в деятельности клиента операций, подлежащих обязательному контролю, подозрительных операций, сведения по которым представлены в уполномоченный орган;

- если Компания получила запрос от уполномоченного органа о предоставлении информации и/или документов о Клиенте и (или) операциях Клиента;

- в случае принятия в отношении Клиента решения об отказе в выполнении его распоряжения о совершении операции / сделки;

- независимо от срока обновления сведений с низкого на средний уровень, или на высокий уровень, или со среднего уровня риска на высокий уровень, если в процессе осуществления внутреннего контроля появились основания, достаточные для пересмотра уровня Риска Клиента;

- независимо от срока обновления сведений с высокого на средний или низкий уровень, или со среднего на низкий уровень, если в процессе осуществления внутреннего контроля появились основания, достаточные для пересмотра уровня Риска Клиента.

7.2.9. В случае признания операций (сделок) клиента подозрительными, в день признания и отправки сообщений в уполномоченный орган, сотрудником КО изменяется «Степень риска» на «высокий». изменения уровня риска фиксируются уполномоченным сотрудником Компании в досье клиента.

8. DUE DILIGENCE OF TRANSACTIONS (KNOW YOUR TRANSACTION, KYT)

8. НАДЛЕЖАЩАЯ ПРОВЕРКА ТРАНЗАКЦИИ (ЗНАЙ СВОЮ ТРАНЗАКЦИЮ KYT)

8.1. Transaction due diligence (Know Your Transaction, KYT) is the second key element after Customer Due Diligence (Know Your Customer,

8.1. Надлежащая проверка транзакции (Знай свою транзакцию KYT) является вторым ключевым элементом после Надлежащей проверки клиента (Знай своего клиента KYC) для защиты бизнеса, соблюдения законодательства Кыргызской Республики и международного законодательства в сфере ПФПД ЛПД и управления рисками.

8.2. Для исполнения сделок с виртуальными активами оператор обмена виртуальных активов получает от клиента на свой текущий (расчетный) банковский счет, свой электронный кошелек, на свой адрес (идентификатор) виртуального кошелька соответственно деньги, электронные деньги, виртуальные активы и передает клиенту в зависимости от вида совершенной сделки с виртуальными активами в качестве встречного предоставления деньги, электронные деньги или виртуальные активы.

8.3. При оказании услуг по покупке и продаже виртуальных активов оператор обмена виртуальных активов использует только безналичный расчет.

8.4. Оператор обмена виртуальных активов совершает следующие сделки с виртуальными активами:

- покупка виртуальных активов за национальную валюту, иностранную валюту, электронные деньги, в том числе международные электронные деньги;

- продажа виртуальных активов за национальную валюту, иностранную валюту, электронные деньги, в том числе международные электронные деньги;

- обмен виртуальных активов одного вида на виртуальные активы другого вида.

8.5. Надлежащая проверка транзакции KYT:

Анализ каждой транзакции на предмет соответствия уровням риска;

Проверка адресов отправителя и получателя на наличие «грязной разметки»;

Выявление подозрительных операций (например, перевод через миксеры или мосты).

8.6. Оператор обмена виртуальных активов применяет меры надлежащей проверки транзакций клиента ко всем клиентам, с учетом ранее проведенной надлежащей проверки клиента и уровня риска клиента.

8.7. К мерам надлежащей проверки транзакций относятся процедуры анализа каждой транзакции на предмет соответствия уровням риска.

8.8. Надлежащая проверка клиентов осуществляется путем проверки адресов отправителя и получателя виртуальных

KYC) for protecting the business, complying with the legislation of the Kyrgyz Republic and international legislation in the field of CFCA/LCP, and risk management.

8.2. To execute transactions with virtual assets, the virtual asset exchange operator receives from the client to its current (settlement) bank account, its electronic wallet, to its address (identifier) of the virtual wallet respectively money, electronic money, virtual assets and transfers to the client, depending on the type of transaction made with virtual assets, as counter-performance, money, electronic money or virtual assets.

8.3. When providing services for the purchase and sale of virtual assets, the virtual asset exchange operator uses only non-cash settlements.

8.4. The virtual asset exchange operator carries out the following transactions with virtual assets:

- purchase of virtual assets for national currency, foreign currency, electronic money, including international electronic money;
- sale of virtual assets for national currency, foreign currency, electronic money, including international electronic money;
- exchange of one type of virtual assets for another type of virtual assets.

8.5. Due diligence of a KYT transaction: Analysis of each transaction for compliance with risk levels;

Checking sender and recipient addresses for the presence of “dirty marking”;

Identification of suspicious operations (for example, transfer through mixers or bridges).

8.6. The virtual asset exchange operator applies customer transaction due diligence measures to all clients, taking into account previously conducted customer due diligence and the client’s risk level.

8.7. Transaction due diligence measures include procedures for analyzing each transaction for compliance with risk levels.

8.8. Customer due diligence is carried out by checking the addresses of the sender and recipient of virtual assets for the presence of “dirty marking.” At the same time, dirty marking means the identification of cryptocurrency assets related to illegal or suspicious activity using analytical data and sanctions lists, through the use of specialized tools for analysis of operations with virtual assets, including analysis of transactions in the blockchain environment, assessment of risks of virtual asset addresses and identification of operations with high-risk addresses recommended by the Financial Market Regulation and Supervision Service under the Ministry of Economy and Commerce of the Kyrgyz Republic,

активов на наличие «грязной разметки». При этом под грязной разметкой понимается идентификация криптовалютных активов, связанных с незаконной или подозрительной деятельностью, используя аналитические данные и санкционные списки, через применение специализированных инструментов анализа операций с виртуальными активами, включая анализ транзакций в блокчейн-среде, оценку рисков адресов виртуальных активов и выявление операций с высокорискованными адресами, рекомендованных Службой регулирования и надзора за финансовым рынком при Министерстве экономики и коммерции Кыргызской Республики, а также другими аналитическими платформами AML проверки, в случае необходимости.

8.9. Оператор обмена виртуальных активов обязан провести проверку адреса кошелька виртуального актива, до предоставления клиенту Услуг обмена виртуальных активов.

8.10. Оператор обмена виртуальных активов обязан проводить анализ каждой транзакции клиента на предмет соответствия уровням риска.

8.11. Оператор обмена виртуальных активов при выявлении подозрительных операций (например, перевод через миксеры или мосты) обязан задокументировать данный факт.

8.12. Для минимизации последствий и защиты Оператор обмена виртуальных активов должен соблюдать следующие шаги:

1. Фиксация транзакции:

Хэш транзакции.

Адреса отправителя и получателя.

Дата, время и сумма транзакции.

2. Получение данных от отправителя:

Получение у отправителя информации о происхождении активов.

Фиксация переписки с отправителем, включая электронные письма, сообщения в мессенджерах и другие способы коммуникации.

3. Создание отчета:

В случае выявления нарушений Оператор обмена виртуальных активов должен подготовить детализированный отчет с описанием выявленных нарушений и приложением данных о транзакции.

8.13. Оператор обмена виртуальных активов должен указать используемые инструменты анализа и результаты проверок.

8.14. Для минимизации рисков Оператор обмена виртуальных активов отправляет и принимает виртуальные активы только с холодных кошельков, зарегистрированных в

as well as other AML verification analytical platforms, if necessary.

8.9. The virtual asset exchange operator is obliged to check the address of the virtual asset wallet before providing the client with Virtual Asset Exchange Services.

8.10. The virtual asset exchange operator is obliged to analyze each client transaction for compliance with risk levels.

8.11. Upon identification of suspicious operations by the virtual asset exchange operator (for example, transfer through mixers or bridges), it is obliged to document this fact.

8.12. To minimize consequences and ensure protection, the virtual asset exchange operator must observe the following steps:

1. Recording of the transaction:

Transaction hash.

Sender and recipient addresses.

Date, time and transaction amount.

2. Obtaining data from the sender:

Obtaining from the sender information about the origin of the assets.

Recording correspondence with the sender, including emails, messages in messengers and other means of communication.

3. Creating a report:

In the event of violations being identified, the virtual asset exchange operator must prepare a detailed report describing the identified violations and attaching transaction data.

8.13. The virtual asset exchange operator must indicate the analytical tools used and the results of the checks.

8.14. To minimize risks, the virtual asset exchange operator sends and receives virtual assets only from cold wallets registered with the authorized body of the Kyrgyz Republic. Each wallet must be verified during the transaction.

8.15. The virtual asset exchange operator is prohibited from carrying out operations with virtual assets, virtual asset wallets having a high level of risks identified as a result of percentage scoring;

it is prohibited to use anonymous wallets, NFTs, prepaid foreign cards, transactions with online casinos and assets with a high level of risk.

уполномоченном органе Кыргызской Республики. Каждый кошелек должен быть проверен во время проведения сделки.

8.15. Оператору обмена виртуальных активов запрещено осуществлять операции с виртуальными активами, кошельками виртуальных активов, имеющими высокий уровень рисков, выявленных в результате процентного скоринга;

запрещено использовать анонимные кошельки, NFT, предоплаченные зарубежные карты, операции с онлайн-казино и активами с высоким уровнем риска.

9. МОНИТОРИНГ

9.1.1. Мониторингу подлежат:

- а. кошельки (идентификаторы) виртуальных активов, используемые Клиентами для продажи виртуальных активов;
- б. кошельки (идентификаторы) виртуальных активов, используемые Клиентами для покупки Виртуальных активов;
- в. отдельные Транзакции – по решению комплаенс-оффисера.

9.1.2. Оператор обмена виртуальных активов использует для целей анализа кошельков Клиентов программное обеспечение-анализатор блокчейна: «Runex» (ПО «Runex»). Указанное ПО базируется на алгоритмах графового анализа для определения связей между кошельками (идентификаторами) Виртуальных активов, эмитированными в определенном блокчейне, и Транзакциями в рамках данного блокчейна, что позволяет выявлять подозрительную активность тех или иных кошельков, в связи с чем каждому из проверяемых через ПО «Runex» кошельков (идентификаторов) Виртуальных активов по результатам проверки присваивается определенный уровень риска (процентный скоринг).

9.1.3. Поскольку Оператор обмена виртуальных активов оказывает услуги в области виртуальных активов, то в связи с этим уполномоченное лицо в сфере ПФПД ЛПД организует и осуществляет постоянный мониторинг в отношении:

- а. подозрительных Транзакций;
- б. Транзакций в пользу физических или юридических лиц из высокорискованных стран, если Клиент при этом сообщил Оператору обмена виртуальных активов данные получателя Виртуальных активов, в результате анализа которых уполномоченное лицо в сфере ПФПД ЛПД установил принадлежность представленных данных лицу

9. MONITORING

9.1.1. The following are subject to monitoring:

- a. wallets (identifiers) of virtual assets used by Clients for the sale of virtual assets;
- b. wallets (identifiers) of virtual assets used by Clients for the purchase of Virtual assets;
- c. individual Transactions – by decision of the compliance officer.

9.1.2. For the purposes of analyzing Clients' wallets, the virtual asset exchange operator uses blockchain analyzer software: "Runex" (Runex software). The said software is based on graph analysis algorithms to determine relationships between wallets (identifiers) of Virtual assets issued in a certain blockchain and Transactions within that blockchain, which makes it possible to identify suspicious activity of certain wallets, in connection with which each wallet (identifier) of Virtual assets checked through the Runex software is assigned a certain risk level (percentage scoring) based on the results of the check.

9.1.3. Since the virtual asset exchange operator provides services in the field of virtual assets, in connection with this the authorized person in the field of CFCA/LCP organizes and carries out constant monitoring in respect of:

- a. suspicious Transactions;
- b. Transactions in favor of individuals or legal entities from high-risk countries, if the Client at the same time informed the virtual asset exchange operator of the data of the recipient of Virtual assets, as a result of the analysis of which the authorized person in the field of CFCA/LCP established that the provided data belongs to a person from a high-risk country (permission of the head is required to continue business relations);
- c. Transactions initiated by individuals who have served punishment for carrying out legalization (laundering) of criminal proceeds, terrorist or extremist activity.

9.1.4. In addition, taking into account the requirements of regulatory legal acts in the field of CFCA/LCP, the virtual asset exchange operator carries out monitoring of Transactions if the criteria established in the following are applicable to them:

из высокорискованной страны (необходимо разрешение руководителя на продолжение деловых отношений);

в. Транзакции, инициируемые физическими лицами, отбывшими наказание за осуществление легализации (отмывания) преступных доходов, террористической или экстремистской деятельности;

9.1.4. Кроме того, учитывая требования нормативных правовых актов в сфере ПФПД ЛПД, Оператор обмена виртуальных активов осуществляет мониторинг Транзакций, если ним применимы критерии, установленные в:

а. Перечне критериев и справочник кодов операций (сделок), подлежащих обязательному контролю, утв. утв. Приказом Государственной службы финансовой разведки при Правительстве Кыргызской Республики от «23» января 2017 г. № 1/нпа;

б. Перечне критериев (признаков) и справочник кодов подозрительных операций (сделок), утв. Приказом Государственной службы финансовой разведки при Правительстве Кыргызской Республики от «23» января 2017 г. № 1/нпа.

9.1.5. Оператор обмена виртуальных активов использует комбинированный способ постоянного мониторинга транзакций, который представляет собой сочетание автоматизированного и ручного способов мониторинга.

9.1.6. Автоматизированный способ мониторинга базируется на ПО «Runex».

9.1.7. Ручной способ мониторинга предполагает организацию и проведение комплаенс офицером аналитики данных, относящихся к Транзакциям, в отношении которых, исходя из применимых критериев, должен быть установлен постоянный мониторинг.

9.1.8. Источником данных для проведения ручного мониторинга являются:

а. архивные сведения о Транзакциях, проведенных через Оператора обмена виртуальных активов;

б. обращения Клиентов в службу клиентской поддержки;

в. детализированные риск-скоринговые отчеты (источники таких отчетов – ПО «Runex»).

9.1.9. Для недопущения проведения через Оператора обмена виртуальных активов операций в целях ПФПД ЛПД уполномоченное лицо в сфере ПФПД ЛПД обеспечивает ознакомление работников с Методическими рекомендациями и рекомендациями ФАТФ по выявлению подозрительных Транзакций.

a. the List of criteria and reference guide of codes of operations (transactions) subject to mandatory control, approved by Order of the State Financial Intelligence Service under the Government of the Kyrgyz Republic dated January 23, 2017 No. 1/npa;

b. the List of criteria (signs) and reference guide of codes of suspicious operations (transactions), approved by Order of the State Financial Intelligence Service under the Government of the Kyrgyz Republic dated January 23, 2017 No. 1/npa.

9.1.5. The virtual asset exchange operator uses a combined method of continuous transaction monitoring, which is a combination of automated and manual monitoring methods.

9.1.6. The automated monitoring method is based on the Runex software.

9.1.7. The manual monitoring method involves organization and conduct by the compliance officer of analytics of data relating to Transactions in respect of which, based on applicable criteria, continuous monitoring must be established.

9.1.8. The source of data for manual monitoring is:

a. archived information on Transactions carried out through the virtual asset exchange operator;

b. Client appeals to customer support service;

c. detailed risk-scoring reports (the source of such reports is the Runex software).

9.1.9. In order to prevent operations through the virtual asset exchange operator for CFCA/LCP purposes, the authorized person in the field of CFCA/LCP ensures familiarization of employees with Methodological Recommendations and FATF recommendations for identifying suspicious Transactions.

9.1.10. If, within the framework of analyzing the Client's activity, the authorized person in the field of CFCA/LCP identifies facts of this Client carrying out Transactions having signs of suspiciousness, then in the said case the compliance officer has the right to:

a. contact the Client to obtain explanations from him confirming the intended purpose or the actual economic meaning of unusual Transactions;

b. organize enhanced monitoring of all Transactions for this Client.

9.1.11. Based on the results of the analysis of suspicious Transactions and the explanations provided by the Client and disclosing the intended purpose or the actual economic meaning of unusual Transactions, the authorized person in the field of CFCA/LCP has the right to apply to the Director for additional instructions on further actions. The Director may at the same time make one of the following decisions:

9.1.10. Если в рамках проведения анализа деятельности Клиента уполномоченным лицом в сфере ПФПД ЛПД будут выявлены факты совершения данным Клиентом Транзакций, имеющих признаки подозрительности, то в указанном случае комплаенс офицер вправе:

а. обратиться к Клиенту для получения от него разъяснений, подтверждающих целевое назначение либо действительный экономический смысл необычных Транзакций;

б. организовать усиленный мониторинг всех Транзакций по данному Клиенту;

9.1.11. По итогам анализа подозрительных Транзакций и разъяснений, представленных Клиентом и раскрывающих целевое назначение либо действительный экономический смысл необычных Транзакций, уполномоченное лицо в сфере ПФПД ЛПД вправе обратиться к Директору для получения дополнительных инструкций о дальнейших действиях. Директор при этом может принять одно из нижеследующих решений:

а. о признании Транзакций, инициированных Клиентом, операциями, подлежащими обязательному контролю и сообщению;

б. о признании необычных Транзакций подозрительными Транзакциями, потенциально инициированными Клиентом в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

в. о необходимости принятия дополнительных мер по изучению необычных Транзакций;

г. о представлении информации о Транзакциях в орган финансовой разведки.

г. процедура применения к Клиенту целевых финансовых санкций и приостановления операций (сделок) Клиента:

9.1.12. Исходя из положений Закона о ПФПД ЛПД, под целевыми финансовыми санкциями Компания подразумевает замораживание любых операций (сделок) и (или) средств Клиентов:

1) если имеются подозрение или достаточные основания подозревать, что средства являются доходом, полученным преступным путем, в том числе от предикатных преступлений, или связаны с легализацией (отмыванием) преступных доходов;

2) если имеются подозрение или достаточные основания подозревать, что средства связаны с финансированием:

а) террористов и экстремистов;

б) террористических и экстремистских организаций (групп);

а. on recognizing Transactions initiated by the Client as operations subject to mandatory control and reporting;

б. on recognizing unusual Transactions as suspicious Transactions potentially initiated by the Client for the purpose of legalization (laundering) of proceeds obtained by criminal means, or financing of terrorism;

с. on the need to take additional measures to study unusual Transactions;

д. on submission of information on Transactions to the financial intelligence authority.

е. procedure for applying targeted financial sanctions to the Client and suspension of the Client's operations (transactions):

9.1.12. Based on the provisions of the Law on CFCA/LCP, by targeted financial sanctions the Company means freezing of any operations (transactions) and/or funds of Clients:

1. if there is suspicion or sufficient grounds to suspect that the funds are proceeds obtained by criminal means, including predicate crimes, or are connected with legalization (laundering) of criminal proceeds;

2. if there is suspicion or sufficient grounds to suspect that the funds are connected with financing of:

a) terrorists and extremists;

b) terrorist and extremist organizations (groups);

c) terrorist and extremist activity;

d) organized groups or criminal communities;

e) proliferation of weapons of mass destruction.

9.1.13. The compliance officer checks the identification data provided by Clients within the framework of undergoing identification and verification procedures through databases (national and international), which allows the Company to identify persons included in:

а. the Consolidated Sanctions List of the Kyrgyz Republic;

б. the Consolidated Sanctions List of the UN Security Council;

с. the List of persons, groups, organizations in respect of whom there is information on their participation in legalization (laundering) of criminal proceeds;

д. the List of individuals who have served punishment for carrying out legalization (laundering) of criminal proceeds, terrorist or extremist activity, as well as for financing this activity;

е. **list of high-risk countries identified by the Financial Intelligence Unit of the Kyrgyz Republic.**

в) террористической и экстремистской деятельности;

г) организованных групп или преступных сообществ;

д) распространения оружия массового уничтожения.

9.1.13. Комплаенс офицер осуществляет проверку идентификационных данных, представленных Клиентами в рамках прохождения процедур идентификации и верификации, через базы данных (национальные и международные), что позволяет Компании выявлять лиц, включенных в:

а. Сводный санкционный перечень Кыргызской Республики;

б. Сводный санкционный перечень Совета Безопасности ООН;

в. Перечень лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов;

г. Перечень физических лиц, отбывших наказание за осуществление легализации (отмывания) преступных доходов, террористической или экстремистской деятельности, а также за финансирование данной деятельности;

д. **Перечень высоко рискованных стран, определенных органом финансовой разведки Кыргызской Республики.**

9.1.14. Исходя из содержания п. 19 ч. 1 ст. 1 и ст. 12 Закона о ПФПД ЛПД, Сводный санкционный перечень Кыргызской Республики и Сводный санкционный перечень Совета Безопасности ООН в совокупности составляют единый Санкционный перечень, учитывающий физических и юридических лиц, группы и организации, в отношении которых имеются сведения об их участии в террористической или экстремистской деятельности и распространении оружия массового уничтожения.

9.1.15. При выявлении достаточного количества совпадений между идентификационными данными Клиента и данными одного либо нескольких подсанкционных лиц, включенных в указанные перечни (далее – «Установленное лицо»), уполномоченное лицо в сфере ПФПД ЛПД принимает необходимые меры реагирования, направленные на ограничение оказания услуг в пользу Установленного лица.

9.1.14. Based on the content of paragraph 19 of part 1 of Article 1 and Article 12 of the Law on CFCA/LCP, the Consolidated Sanctions List of the Kyrgyz Republic and the Consolidated Sanctions List of the UN Security Council together constitute a single Sanctions List taking into account individuals and legal entities, groups and organizations in respect of whom there is information on their participation in terrorist or extremist activity and proliferation of weapons of mass destruction.

9.1.15. When a sufficient number of matches are identified between the Client's identification data and the data of one or more sanctioned persons included in the said lists (hereinafter, the "Identified Person"), the authorized person in the field of CFCA/LCP takes the necessary response measures aimed at restricting the provision of services in favor of the Identified Person.

10. RISKS WHEN CONDUCTING TRANSACTIONS WITH VIRTUAL ASSETS

10.1.1. In its activities, the virtual asset exchange operator may encounter risks characteristic only of activities with virtual assets:

- Risk associated with the use of distributed ledgers;

10. РИСКИ ПРИ ПРОВЕДЕНИИ ОПЕРАЦИЙ С ВИРТУАЛЬНЫМИ АКТИВАМИ

10.1.1. Оператор обмена виртуальных активов в своей деятельности может столкнуться с рисками характерными только для деятельности с виртуальными активами:

Риск, связанный с использованием распределенных реестров;

Риск, связанный с трансграничным характером операций с виртуальными активами;

Риск, связанный с технологической сложностью операций и возможной псевдонимностью участников операций;

Риск, связанный с использованием сервисов анонимизации (миксеры);

Риск, связанный с использованием смены сетей (chain hopping);

Риск, связанный с использованием кроссчейн-мостов;

Риск, связанный с использованием DeFi-платформ.

10.1.2. Система распределенных реестров (DLT) — это технология децентрализованного хранения данных, при которой база данных синхронизируется и реплицируется между множеством узлов (компьютеров) без единого администратора. Она обеспечивает прозрачность, неизменность данных и высокую безопасность, используя криптографические методы и алгоритмы консенсуса для проверки транзакций. Блокчейн=системе распределенных реестров (DLT).

10.1.3. Использование распределенных реестров (DLT) и виртуальных активов несет риски высокой волатильности, технологических сбоев, уязвимости смарт-контрактов, а также сложности правового регулирования. Трансграничность усложняет контроль, псевдонимность затрудняет идентификацию участников, а техническая сложность повышает риски кражи активов и легализации преступных доходов.

10.1.4. Использование сервисов анонимизации (миксеры), chain hopping (смена сетей), кроссчейн-мостов и DeFi-платформ позволяет значительно усложнить отслеживание криптоактивов, перемещая их между блокчейнами и перемешивая с другими средствами. Технологии обеспечивают высокую приватность, но повышают риски мошенничества и регуляризации. Ключевые инструменты включают:

- Risk associated with the cross-border nature of operations with virtual assets;

- Risk associated with the technological complexity of operations and the possible pseudonymity of participants in operations;

- Risk associated with the use of anonymization services (mixers);

- Risk associated with the use of chain hopping;

- Risk associated with the use of cross-chain bridges;

- Risk associated with the use of DeFi platforms.

10.1.2. A distributed ledger system (DLT) is a technology of decentralized data storage in which a database is synchronized and replicated among many nodes (computers) without a single administrator. It ensures transparency, immutability of data and high security using cryptographic methods and consensus algorithms for verifying transactions. Blockchain = distributed ledger system (DLT).

10.1.3. The use of distributed ledgers (DLT) and virtual assets carries risks of high volatility, technological failures, vulnerabilities of smart contracts, as well as complexity of legal regulation. Cross-border nature complicates control, pseudonymity complicates identification of participants, and technical complexity increases the risks of theft of assets and legalization of criminal proceeds.

10.1.4. The use of anonymization services (mixers), chain hopping, cross-chain bridges and DeFi platforms makes it possible to significantly complicate the tracking of crypto assets by moving them between blockchains and mixing them with other funds. The technologies ensure high privacy, but increase the risks of fraud and regularization. Key tools include:

Anonymization services (mixers): mix funds to break the link between sender and recipient.

Chain Hopping: rapid movement of assets between different blockchains (for example, BTC into ETH) to mask traces.

Bridges: protocols allowing tokens to be moved between blockchains by locking/burning them in one network and issuing “wrapped” tokens in another.

DeFi platforms: decentralized exchanges (DEX) and protocols functioning without intermediaries, which ensures transparency but reduces centralized control.

These methods may be used to bypass the transparency of public blockchains, creating new approaches to ensuring confidentiality of assets, but they may also be used to conceal illegal transactions.

10.1.5. Main methods of identifying high-risk operations with VA.

Сервисы анонимизации (миксеры): смешивают средства для разрыва связи между отправителем и получателем.

Chain Hopping: Быстрое перемещение активов между различными блокчейнами (например, BTC в ETH) для маскировки следов.

Мосты (Bridges): Протоколы, позволяющие перемещать токены между блокчейнами путем их блокировки/сжигания в одной сети и выпуска «обернутых» (wrapped) токенов в другой.

DeFi-платформы:

Децентрализованные биржи (DEX) и протоколы, функционирующие без посредников, что обеспечивает прозрачность, но снижает централизованный контроль.

Эти методы могут использоваться для обхода прозрачности публичных блокчейнов, создавая новые подходы к обеспечению конфиденциальности активов, но они также могут использоваться для сокрытия незаконных транзакций.

10.1.5. Основные методы выявления операций повышенного риска с ВА

Выявление подозрительных транзакций базируется на сочетании автоматизированных инструментов и аналитических методик.

Ключевые методы выявления:

- Анализ поведения и транзакционных паттернов: Выявление нетипичных для клиента схем, таких как:

Цепочки "перескока" (Chain Hopping): Быстрая конвертация актива из одной сети в другую без экономической цели.

Транзакции "структурирования": Разбиение крупной суммы на множество мелких транзакций чуть ниже порога отчетности.

Взаимодействие с высокорисковыми сервисами: Отправка средств на адреса, идентифицированные как миксеры, или взаимодействие со смарт-контрактами DEX, не требующими KYC.

- Использование инструментов блокчейн-аналитики:

Скрининг адресов: Проверка кошельков клиентов при установлении деловых отношений и в процессе мониторинга на наличие связей с мошенническими схемами, даркнет-маркетами или санкционными списками, а также при проведении любой транзакции, используя АМЛ платформу, выбранную регулятором.

Кластерный анализ: Выявление принадлежности нескольких, казалось бы, несвязанных адресов одному лицу или группе.

Identification of suspicious transactions is based on a combination of automated tools and analytical methods.

Key identification methods:

Analysis of behavior and transaction patterns: Identification of schemes atypical for the client, such as:

Chain Hopping: rapid conversion of an asset from one network into another without economic purpose.

Structuring transactions: breaking a large amount into many small transactions just below the reporting threshold.

Interaction with high-risk services: sending funds to addresses identified as mixers, or interaction with DEX smart contracts that do not require KYC.

Use of blockchain analytics tools:

Address screening: checking client wallets when establishing business relations and in the monitoring process for links with fraudulent schemes, darknet markets or sanctions lists, as well as when conducting any transaction, using the AML platform selected by the regulator.

Cluster analysis: identification of the affiliation of several seemingly unrelated addresses to one person or group.

Analysis of source of funds: tracing the path of funds several "hops" back to find out whether they came from a mixer or from a wallet associated with criminal activity.

10.1.6. Procedure for analyzing operations.

After suspicious activity is identified, an investigation process integrated into the general CFCA/LCP system is launched.

10.1.7. Initial qualification:

Automatic assignment of a risk score to a transaction or client based on configured rules and analytics data.

10.1.8. In-depth review

Request from the client for explanations and supporting documents regarding the purpose of the transaction and the source of funds. Parallel analysis of the transaction, smart contract and other actions occurring directly within the blockchain, (this data is recorded in a distributed ledger that is impossible to alter or delete, which ensures transparency and security) to verify the client's words.

10.1.9. Forming conclusions

Collection of an evidentiary base (transaction hashes, screenshots, analytics logs), documentation of conclusions and decision-making on further actions.

10.10.1. Risks by service type and methods for identifying them Different technologies carry specific risks, which requires the application of differentiated control methods.

Анализ происхождения средств: Прослеживание пути средств на несколько "шагов" назад (hop analysis) для выяснения, не поступили ли они из миксера или с кошелька, связанного с преступной деятельностью.

10.1.6. Порядок анализа операций

После выявления подозрительной активности запускается процесс расследования, интегрированный в общую систему ПФПД ЛПД.

10.1.7. Первичная квалификация:

Автоматическое присвоение рискового балла (risk scoring) транзакции или клиенту на основе настроенных правил и данных аналитики.

10.1.8. Углубленная проверка

Запрос у клиента пояснений и подтверждающих документов о цели транзакции и происхождении средств. Параллельный анализ транзакции, смарт-контракта и других действий, происходящих непосредственно внутри блокчейна, (эти данные записываются в распределенном реестре, который невозможно изменить или удалить, что обеспечивает прозрачность и безопасность) для проверки слов клиента.

10.1.9. Формирование выводов

Сбор доказательной базы (хэши транзакций, скриншоты, логи аналитики), документирование выводов и принятие решения о дальнейших действиях.

10.10.1. Риски по типам сервисов и методы их выявления

Разные технологии несут в себе специфические риски, что требует применения дифференцированных методов контроля.

Анонимные кошельки

Основные риски для Оператора обмена ВА:

Отсутствие информации о владельце кошелька, невозможность применения санкционного комплаенса к контрагенту, высокий риск получения средств с нелегальных источников.

Методы выявления и анализа:

Внедрение риск-ориентированного подхода к транзакциям с некастодиальными кошельками (например, лимиты на вывод, требование дополнительной верификации). Использование аналитики для "отмывания" репутации кошелька.

Криптомиксеры

Основные риски для Оператора обмена ВА:

Преднамеренное разрыв связи между адресом отправителя и получателя. Прямое нарушение принципов прозрачности. Активно

Anonymous wallets

Main risks for the VA Exchange Operator:

absence of information about the wallet owner, impossibility of applying sanctions compliance to the counterparty, high risk of receiving funds from illegal sources.

Methods of identification and analysis: implementation of a risk-based approach to transactions with non-custodial wallets (for example, withdrawal limits, requirement of additional verification). Use of analytics for "laundering" the wallet's reputation.

Crypto mixers

Main risks for the VA Exchange Operator:

deliberate breaking of the connection between the sender's and recipient's address. Direct violation of the principles of transparency. Actively used for laundering funds after hacks.

Methods of identification and analysis:

adding mixer addresses to "blacklists" (blocking incoming/outgoing transactions). Behavioral analysis: identification of deposits with a fixed time delay and subsequent withdrawal to new addresses.

Decentralized platforms (DEX)

Main risks for the VA Exchange Operator:

absence of KYC on the protocol itself, possibility of bypassing blocks through interaction with smart contracts, difficulty in tracking liquidity and real beneficiaries.

Methods of identification and analysis:

monitoring the interaction of client wallets with known DEX contracts. Analysis for "laundering" of funds through liquidity pools where funds are mixed with legitimate ones.

Cross-chain transfers

Main risks for the VA Exchange Operator:

use of bridges to "break" the traceability chain at blockchain boundaries. Analytical tools often have delays in supporting new bridges.

Methods of identification and analysis:

tracing the path of funds through specialized protocols (blockchain explorers) supporting multiple networks. Paying attention to wrapped tokens (for example, wBTC), which are a marker of a cross-chain transfer.

10.10.2. To implement the described measures, the VA Exchange Operator builds a technological and process basis.

Blockchain analytics platforms: the blockchain analytics AML platform Raneks selected by the authorized body, additional solutions Chainalysis, Elliptic, TRM Labs or Competent BlockSec. Implementation of these tools makes it possible to automate address screening, visualize the movement of funds and receive up-to-date data on risky entities.

используются для отмывания средств после взломов.

Методы выявления и анализа:

Внесение адресов миксеров в "черные списки" (блокировка входящих/исходящих транзакций).

Поведенческий анализ: выявление депозитов с фиксированной временной задержкой и последующим выводом на новые адреса.

Децентрализованные платформы (DEX)

Основные риски для Оператора обмена ВА:

Отсутствие KYC на самом протоколе, возможность обхода блокировок через взаимодействие со смарт-контрактами, сложность отслеживания ликвидности и реальных бенефициаров.

Методы выявления и анализа:

Мониторинг взаимодействия клиентских кошельков с известными контрактами DEX. Анализ на предмет "отмывания" средств через пулы ликвидности, где средства смешиваются с законными.

Межсетевые переводы (Cross-chain)

Основные риски для Оператора обмена ВА:

Использование мостов (bridges) для "обрыва" цепочки отслеживания на границе блокчейнов. Аналитические инструменты часто имеют задержки в поддержке новых мостов.

Методы выявления и анализа:

Прослеживание пути средств через специализированные протоколы (blockchain explorers), поддерживающие несколько сетей. Обращение внимания на wrapped-токены (например, wBTC), которые являются маркером межсетевого перевода.

10.10.2. Для реализации описанных мер Оператор обмена ВА выстраивает технологическую и процессную базу.

Платформы блокчейн-аналитики: выбранная уполномоченным органом АМЛ платформа блокчейн аналитики Ранекс, дополнительные решения Chainalysis, Elliptic, TRM Labs или Competent BlockSec. Внедрение этих инструментов позволяет автоматизировать скрининг адресов, визуализировать движение средств и получать актуальные данные о рискованных сущностях.

Соблюдение "Travel Rule": Внедрение технических решений (например, TRISA, OpenVASP) для безопасной передачи данных об отправителе и получателе перевода между поставщиками услуг виртуальных активов, что критически важно для противодействия анонимным переводам.

Compliance with the "Travel Rule": implementation of technical solutions (for example, TRISA, OpenVASP) for secure transfer of data on the sender and recipient of a transfer between virtual asset service providers, which is critically important for countering anonymous transfers.

Personnel training: regular improvement of the qualifications of compliance employees regarding new money laundering schemes.

Independent audit of the internal control system: periodic verification of the effectiveness of measures taken by external audit forces to identify "blind spots" in the monitoring system.

11. POLICY ON MANAGING RISKS ASSOCIATED WITH CRYPTO MIXERS

Обучение персонала: регулярное повышение квалификации сотрудников комплаенс в части новых схем отмывания денег.

Независимый аудит системы внутреннего контроля: периодическая проверка эффективности принятых мер силами внешнего аудита для выявления "слепых зон" в системе мониторинга.

11. ПОЛИТИКА ПО УПРАВЛЕНИЮ РИСКАМИ, СВЯЗАННЫМИ С КРИПТОМИКСЕРАМИ

11.1. Цель: минимизация правовых, репутационных и регуляторных рисков Оператора обмена ВА, связанных с непреднамеренным обслуживанием клиентов, использующих криптомиксеры для отмывания доходов, полученных преступным путем, или финансирования терроризма.

Область применения: настоящая Политика распространяется на все сервисы Оператора обмена ВА и применяется ко всем клиентам при проведении входящих и исходящих транзакций с виртуальными активами.

Определение: Под криптомиксерами понимаются сервисы (централизованные или децентрализованные протоколы), предназначенные для разрыва связи между адресом отправителя и получателя путем смешивания криптовалютных средств множества пользователей.

11.2. Нормативная база и риск-аппетит

Риск-аппетит: оператор обмена ВА придерживается политики нулевой толерантности к прямым транзакциям с адресами криптомиксеров, включенными в санкционные списки (например, Tornado Cash, по спискам OFAC). Опосредованная связь (через 1-2 хопа) является основанием для проведения усиленной проверки (EDD).

Основание:

Рекомендации FATF (особенно в части применения Риск-ориентированного подхода). Требования законодательства Кыргызской Республики в сфере ПФПД ЛПД.

Санкционные списки.

11.3. Идентификация и выявление транзакций, связанных с миксерами

Для выявления используются следующие методы:

Автоматизированный скрининг адресов:

Все адреса кошельков клиентов и контрагентов проверяются через платформу блокчейн-аналитики Ранекс Кей Джи на предмет прямых совпадений с базой данных известных миксеров.

Поведенческий анализ:

11.1. Purpose: minimization of legal, reputational and regulatory risks of the VA Exchange Operator associated with unintentional servicing of clients using crypto mixers for laundering proceeds obtained by criminal means or financing terrorism. Scope: this Policy applies to all services of the VA Exchange Operator and applies to all clients when conducting incoming and outgoing transactions with virtual assets.

Definition: Crypto mixers mean services (centralized or decentralized protocols) intended to break the link between the sender's and recipient's address by mixing the cryptocurrency funds of many users.

11.2. Regulatory framework and risk appetite Risk appetite: the VA exchange operator adheres to a zero-tolerance policy for direct transactions with crypto mixer addresses included in sanctions lists (for example, Tornado Cash under OFAC lists). Indirect connection (through 1–2 hops) is grounds for enhanced due diligence (EDD).

Basis:

- FATF Recommendations (especially regarding application of the Risk-Based Approach).

- Requirements of the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

- Sanctions lists.

11.3. Identification and detection of transactions related to mixers

The following methods are used for detection:

Automated address screening:

All wallet addresses of clients and counterparties are checked through the Raneks KG blockchain analytics platform for direct matches with the database of known mixers.

Behavioral analysis:

Monitoring of the transaction structure: Identification of patterns of multiple inputs from different users and subsequent sending to new addresses with a fixed time delay.

Analysis of amounts: Recording operations with non-standard amounts characteristic of the work of mixers (for example, frequent deposits just below the thresholds of automatic screening).

Threat sources:

Monitoring news about hacks (when hackers send stolen funds into mixers). Addresses of such hackers are promptly loaded into stop-lists.

11.4. Due diligence procedures and decision-making

Red level (Prohibition)

- Direct interaction (input/output) with a mixer address from sanctions lists.

- Proven participation in a money laundering scheme after major hacks.

Мониторинг структуры транзакции: Выявление паттернов множественных входов от разных пользователей и последующей отправки на новые адреса с фиксированной временной задержкой.

Анализ сумм: Фиксация операций с нестандартными суммами, характерными для работы миксеров (например, частые депозиты чуть ниже порогов автоматического скрининга).

Источники угроз:

Мониторинг новостей о взломах (когда хакеры отправляют украденные средства в миксеры). Адреса таких хакеров оперативно загружаются в стоп-листы.

11.4. Процедуры надлежащей проверки и принятие решений

Красный уровень (Запрет)

1. Прямое взаимодействие (вход/выход) с адресом миксера из санкционных списков.
2. Доказанное участие в схеме отмыwania средств после громких взломов.

Меры реагирования

Немедленная блокировка транзакции.

Замораживание средств (при технической возможности).

Подача СПО в ГСФР.

Расторжение деловых отношений.

Желтый уровень (Усиленный контроль)

1. Транзакции с адресами, имеющими опосредованную связь с миксерами (через 1-2 промежуточных кошелька).
2. Подозрение на использование DEX или мостов (bridges) сразу после вывода из миксера.

Меры реагирования

Запрос EDD: Требование у клиента подтверждения источника средств (документы, скриншоты бирж, подтверждение легального заработка).

Проведение углубленного анализа (риск-скоринг).

Зеленый уровень (Мониторинг)

Отсутствие связей с миксерами, прозрачная история транзакций клиента.

Меры реагирования

Стандартный мониторинг.

11.5. Скрининг взаимодействия с децентрализованными протоколами (DeFi)

Учитывая, что современные миксеры часто маскируются под DeFi-протоколы:

1. Анализ смарт-контрактов: При выявлении взаимодействия клиента со сложными смарт-контрактами, комплаенс офицер Оператора обмена ВА обязан проверить функционал контракта (является ли он тумблером).

Response measures

Immediate blocking of the transaction.

Freezing of funds (where technically possible).

Submission of an STR to the SFRS.

Termination of business relations.

Yellow level (Enhanced control)

1. Transactions with addresses having an indirect connection with mixers (through 1–2 intermediate wallets).

2. Suspicion of use of DEX or bridges immediately after withdrawal from the mixer.

Response measures

EDD request: requiring from the client confirmation of source of funds (documents, exchange screenshots, confirmation of lawful earnings).

Conducting in-depth analysis (risk scoring).

Green level (Monitoring)

No connections with mixers, transparent history of the client's transactions.

Response measures

Standard monitoring.

11.5. Screening of interaction with decentralized protocols (DeFi)

Taking into account that modern mixers are often disguised as DeFi protocols:

1. Smart contract analysis: upon detecting the client's interaction with complex smart contracts, the compliance officer of the VA Exchange Operator is obliged to check the functionality of the contract (whether it is a tumbler).

2. Blocking at the RPC node level: if available, or in case of achieving technical capability, the VA Exchange Operator may block interaction with contract addresses identified as mixers at the level of its infrastructure node.

11.6. Procedure of actions and division of responsibility

1. Employee of the VA operations department:

Daily monitoring of system alerts.

Checking of "green" and "yellow" incidents of low complexity.

2. Compliance officer:

Analysis of "red" incidents.

Decision-making on submission of an STR and interaction with the SFRS.

Request to the head of the VA Exchange Operator to decide on refusal to service the client.

3. IT specialist:

Technical support for freezing of funds (if applicable to the architecture of the VA Exchange Operator's wallet).

Updating lists of blocked addresses.

11.7. Interaction with the SFRS and reporting

1. Suspicious transaction report (STR): any "red level" transaction is

2. Блокировка на уровне RPC узла: При наличии, или в случае достижения технической возможности, Оператор обмена ВА может заблокировать взаимодействие с адресами контрактов, идентифицированными как миксеры, на уровне своего инфраструктурного узла.

11.6 Порядок действий и разграничение ответственности

1. Сотрудник отдела операций С ВА: Ежедневный мониторинг тревожных сигналов системы.

Проверка "зеленых" и "желтых" инцидентов низкой сложности.

2. Комплаенс офицер:

Анализ "красных" инцидентов.

Принятие решения о подаче СПО и взаимодействии с ГСФР.

Запрос руководителю Оператора обмена ВА о принятии решения об отказе в обслуживании клиента.

3. Ай Ти специалист:

Техническая поддержка заморозки средств (если применимо к архитектуре кошелька Оператора обмена ВА).

Обновление списков заблокированных адресов.

11.7. Взаимодействие с ГСФР и отчетность

1. Сообщение о подозрительной операции (СПО): Любая транзакция "красного" уровня, представляется в орган финансовой разведки в течение пяти часов с момента признания в установленном порядке операции (сделки) подозрительной.

2. Запрет на информирование: строго запрещено уведомлять клиента о том, что в отношении него направлено СПО.

11.8. Обучение персонала

1. Ежегодные тренинги: Проведение занятий для сотрудников Front-office (поддержка клиентов) и комплаенс по обновленным методам маскировки транзакций через миксеры и новые адреса таких сервисов.

11.9. Пересмотр политики

Настоящая Политика подлежит пересмотру в случае появления новых значимых регуляторных требований или принципиально новых технологий анонимизации.

12. ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ ОПЕРАЦИЙ С НЕКАСТОДИАЛЬНЫМИ КОШЕЛЬКАМИ

12.1.1 Оператор обмена виртуальных активов в своей деятельности с некастодиальными кошельками:

применяет усиленные меры KYC/AML;

submitted to the financial intelligence authority within five hours from the moment the operation (transaction) is recognized in the established manner as suspicious.

2. Prohibition on informing: it is strictly prohibited to notify the client that an STR has been sent in respect of him.

11.8. Personnel training

1. Annual trainings: conducting classes for Front-office employees (client support) and compliance on updated methods of masking transactions through mixers and new addresses of such services.

11.9. Review of the policy
This Policy is subject to review in case of emergence of new significant regulatory requirements or fundamentally new anonymization technologies.

12. POLICY FOR MANAGING RISKS OF OPERATIONS WITH NON-CUSTODIAL WALLETS

12.1.1 In its activities with non-custodial wallets, the virtual asset exchange operator:

applies enhanced KYC/AML measures;

uses blockchain analytics to verify the origin of funds and identify "dirty" assets (AML screening);

assesses counterparty risks, including verification of their licenses, AML procedures, mandatory exchange of information on beneficial owners (sender and recipient) in cross-border transfers between the virtual asset exchange operator and the counterparty-VASP.

12.1.2. Risks of non-custodial wallets:

The virtual asset exchange operator, when conducting transactions with non-custodial wallets, uses analytical platform tools for AML verification recommended by the authorized body

использует блокчейн-аналитику для проверки происхождения средств и выявления «грязных» активов (AML-скрининг);

оценивает риски контрагентов, включая проверку их лицензий, AML-процедур, обязательный обмен информацией о бенефициарных владельцах

(отправителе и получателе) при трансграничных переводах между Оператором обмена виртуальных активов и контрагентом-ПУВА.

12.1.2. Риски некастодиальных кошельков:

Оператор обмена виртуальных активов при проведении транзакций с некастодиальными кошельками использует аналитические платформы инструменты AML проверки рекомендованные уполномоченным органом Кыргызской Республики для оценки риска контрагента (риск-скоринг адреса);

Идентифицирует пользователя: при превышении лимитов транзакций проводит процедуры подтверждения владения кошельком (например, подпись сообщения или совершение микротранзакции);

Мониторит в реальном времени: оперативно выявляет подозрительную активность и замораживает средства при обнаружении связи с даркнетом, миксерами или санкционными адресами;

Взаимодействует с ПУВА (Криптовбиржи, операторы обмена виртуальных активов):

Перед установлением корреспондентских отношений или проведением крупных сделок проводит проверку ПУВА: наличие лицензии, адекватность их внутренней AML-политики.

Проводит обязательный обмен информацией о бенефициарных владельцах (отправителе и получателе) при трансграничных переводах между ПУВА.

Регулярно направляет СПО в ГСФР при Министерстве финансов Кыргызской Республики о подозрительных транзакциях, о пороговых суммах.

Данная политика направлена на снижение операционных рисков и предотвращение использования виртуальных активов в отмывании денег.

13. ОПЕРАЦИИ (СДЕЛКИ), ПОДЛЕЖАЩИЕ КОНТРОЛЮ И СООБЩЕНИЮ

13.1.1. Оператором обмена виртуальных активов определяется порядок проверки деятельности клиентов на предмет наличия критериев и признаков, свидетельствующих о

of the Kyrgyz Republic to assess counterparty risk (address risk scoring);

Identifies the user: when transaction limits are exceeded, carries out wallet ownership confirmation procedures (for example, signature of a message or making a microtransaction);

Monitors in real time: promptly detects suspicious activity and freezes funds when a connection with darknet, mixers or sanctioned addresses is detected;

Interacts with VASPs (Crypto exchanges, virtual asset exchange operators):

Before establishing correspondent relations or conducting major transactions, it checks the VASP: presence of a license, adequacy of their internal AML policy.

Conducts mandatory exchange of information on beneficial owners (sender and recipient) in cross-border transfers between VASPs.

Regularly sends STRs to the SFRS under the Ministry of Finance of the Kyrgyz Republic on suspicious transactions, on threshold amounts.

This policy is aimed at reducing operational risks and preventing the use of virtual assets in money laundering.

13. OPERATIONS (TRANSACTIONS) SUBJECT TO CONTROL AND REPORTING

13.1.1. The virtual asset exchange operator determines the procedure for checking clients' activities for the presence of criteria and signs indicating the possible financing of criminal activity and legalization (laundering) of criminal proceeds established by the regulatory legal acts of the Kyrgyz Republic. For these purposes, the VA Exchange Operator conducts monitoring of its business relations with clients on a permanent basis, which provides for the following measures: study of transactions carried out on the client's account/account record in order to make sure that the client's activity corresponds to the information available to the VA Exchange Operator about the client, his business and the risk level for this client; if necessary, clarification of the origin of the funds received into the client's account;

возможном осуществлении финансирования преступной деятельности и легализации (отмывания) преступных доходов, установленных нормативными правовыми актами Кыргызской Республики. В этих целях Оператор обмена ВА проводит мониторинг своих деловых отношений с клиентами на постоянной основе, который предусматривает следующие мероприятия: изучение проведенных операций по счету/учетной записи клиента, чтобы убедиться, что деятельность клиента соответствует информации, имеющейся у Оператора обмена ВА о клиенте, его бизнесе и уровне риска по данному клиенту; в случае необходимости выяснение происхождения денежных средств, поступивших на счет клиента; анализ всех сложных или необычайно крупных операций, которые не имеют очевидной или видимой экономической, или законной цели; фиксирование и документирование всей полученной информации Компании и в случае необходимости передача данной информации в орган финансовой разведки.

a. Операция (сделка) с денежными средствами, или иным имуществом, которая является подозрительной и подлежит сообщению в орган финансовой разведки.

b. К операциям (сделкам), подлежащим контролю и сообщению, относятся следующие операции (сделки):

13.1.2. подозрительные операции (сделки) в следующих случаях:

a) если имеются подозрение или достаточные основания подозревать, что средства являются доходом, полученным преступным путем, в том числе от предикатных преступлений, или связаны с легализацией (отмыванием) преступных доходов;

b) если имеются подозрение или достаточные основания подозревать, что средства связаны с финансированием:

- террористов и экстремистов;
- террористических и экстремистских организаций (групп);
- террористической и экстремистской деятельности;
- организованных групп или преступных сообществ;
- распространением оружия массового уничтожения.

c) сообщение о подозрительной операции (сделке), включая о попытке совершения подозрительной операции (сделки), должно направляться независимо от суммы,

analysis of all complex or unusually large operations that have no obvious or visible economic or lawful purpose;

recording and documenting all information received by the Company and, if necessary, transfer of this information to the financial intelligence authority.

a. An operation (transaction) with monetary funds or other property that is suspicious and is subject to reporting to the financial intelligence authority.

b. The following operations (transactions) относятся к операциям (сделкам) subject to control and reporting:

13.1.2. suspicious operations (transactions) in the following cases:

a) if there is suspicion or sufficient grounds to suspect that the funds are proceeds obtained by criminal means, including from predicate crimes, or are connected with the legalization (laundering) of criminal proceeds;

b) if there is suspicion or sufficient grounds to suspect that the funds are connected with the financing of:

- terrorists and extremists;
- terrorist and extremist organizations (groups);
- terrorist and extremist activity;
- organized groups or criminal communities;
- proliferation of weapons of mass destruction.

c) a report on a suspicious operation (transaction), including an attempt to carry out a suspicious operation (transaction), must be sent regardless of the amount of the completed or being completed operation (transaction);

d) the Company familiarizes itself with the “Methodological Guidelines for Identifying Suspicious Operations (Transactions) Related to Virtual Assets” from open sources published in the manner established by the Cabinet of Ministers of the Kyrgyz Republic;

e) a report on a suspicious operation (transaction) shall be submitted to the financial intelligence authority within five hours from the moment the operation (transaction) is recognized in the established manner as suspicious;

f) a report on an operation (transaction) with cash and non-cash monetary funds in an amount equal to or exceeding the threshold amount shall be submitted within three working days from the date of completion of such operation (transaction).

13.1.3. operations (transactions) with individuals or legal entities from high-risk countries. The list of operations (transactions) with individuals or legal entities from high-risk countries subject to reporting to the financial intelligence authority, within two working days from the date of its completion;

совершенной или совершаемой операции (сделки);

d) с «Методическими указаниями по выявлению подозрительных операций (сделок), связанных с виртуальными активами» Компания ознакамливается из открытых источников, публикуемых в порядке, установленном Кабинетом Министров Кыргызской Республики;

e) сообщение о подозрительной операции (сделке) представляется в орган финансовой разведки в течение пяти часов с момента признания в установленном порядке операции (сделки) подозрительной;

f) сообщение об операции (сделке) с наличными и безналичными денежными средствами на сумму, равную или превышающую пороговую сумму, - в течение трех рабочих дней со дня совершения такой операции (сделки).

13.1.3. операции (сделки) с физическими или юридическими лицами из высокорискованных стран. Перечень операций (сделок) с физическими или юридическими лицами из высокорискованных стран, подлежащих сообщению в орган финансовой разведки, в течение двух рабочих дней со дня ее совершения;

13.1.4. операции (сделки), совершенные физическим лицом, отбывшим наказание за осуществление легализации (отмывания) преступных доходов, террористической или экстремистской деятельности, а также за финансирование такой деятельности, в течение двух рабочих дней со дня их совершения;

13.2. До начала осуществления новых видов услуг или операций Оператором обмена ВА должны быть выявлены и оценены все возможные риски, касающиеся данной услуги или операции, в целях противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов.

13.3. Оператор обмена ВА обязан принять необходимые меры с целью проверки наличия в отношении клиента, бенефициарного владельца сведений об их участии в террористической или экстремистской деятельности и распространении оружия массового уничтожения, а также легализации (отмывании) преступных доходов.

Указанные сведения содержатся в Санкционном перечне, а также Перечне лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов,

13.1.4. operations (transactions) carried out by an individual who has served a sentence for legalization (laundering) of criminal proceeds, terrorist or extremist activity, as well as for financing such activity, within two working days from the date of their completion;

13.2. Before the commencement of new types of services or operations by the VA Exchange Operator, all possible risks relating to such service or operation must be identified and assessed for the purpose of countering the financing of criminal activity and the legalization (laundering) of criminal proceeds.

13.3. The VA Exchange Operator is obliged to take the necessary measures in order to verify the existence, with respect to the client and beneficial owner, of information about their participation in terrorist or extremist activity and proliferation of weapons of mass destruction, as well as legalization (laundering) of criminal proceeds. The said information is contained in the Sanctions List, as well as the List of persons, groups, organizations in respect of whom there is information about their participation in legalization (laundering) of criminal proceeds, the authority responsible for the formation and updating of which is the financial intelligence authority.

13.4. Employees of the structural subdivisions of the VA Exchange Operator carrying out identification and verification of clients, and identification of operations having signs of suspicious operations, in accordance with the procedure determined by the Company's internal normative documents, must inform the authorized person for CFCA/LCP of all cases of identified operations having signs of suspicious operations.

14. PROCEDURE FOR SUBMISSION OF INFORMATION AND DOCUMENTS TO

ответственным за формирование и обновление которых является орган финансовой разведки.

13.4. Сотрудники структурных подразделений Оператора обмена ВА, осуществляющие идентификацию и верификацию клиентов, и выявление операций, имеющих признаки подозрительных операций, в соответствии с порядком, определенным ВНД Компании, должны информировать уполномоченное лицо по ПФПД ЛПД о всех случаях выявленных операций, имеющих признаки подозрительных операций.

14. ПОРЯДОК ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ И ДОКУМЕНТОВ В ОРГАН ФИНАНСОВОЙ РАЗВЕДКИ

14.1. Для предоставления информации и документов в орган финансовой разведки Компания обязана подключиться к защищенному электронному каналу связи (ЗЭКС) с ГСФР, заключить Соглашение об обмене информацией, сообщениями и документами в электронном виде по защищенному каналу связи и получить доступ к закрытой части сайта финансовой разведки с целью доступа к Перечню физических лиц, отбывших наказание за осуществление легализации (отмывания) преступных доходов, террористической или экстремистской деятельности, а также за финансирование данной деятельности, к Перечню лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов, а также к Реестру должностей национальных публичных должностных лиц.

14.2. Компания для отправки сообщений о подозрительных операциях (сделках) органу финансовой разведки устанавливает программное обеспечение для шифрования сообщений АРМ ФУС.

14.3. Компания представляет органу финансовой разведки запрашиваемую информацию или документы в сроки, установленные в письменном запросе органа финансовой разведки.

14.3.1. Компания в течение десяти рабочих дней с даты получения запроса обязана представлять соответствующему проверяющему органу запрашиваемую информацию или документы, необходимые для выполнения функций проверяющих органов.

14.3.2. Информация и документы, а также базы данных органа финансовой разведки являются конфиденциальными и защищаются в установленном порядке.

THE FINANCIAL INTELLIGENCE AUTHORITY

14.1. In order to submit information and documents to the financial intelligence authority, the Company shall connect to a secure electronic communication channel (SECC) with the SFRS, conclude an Agreement on the exchange of information, messages and documents in electronic form via a secure communication channel, and obtain access to the closed part of the website of the financial intelligence authority for the purpose of access to the List of individuals who have served a sentence for legalization (laundering) of criminal proceeds, terrorist or extremist activity, as well as for financing such activity, to the List of persons, groups, organizations in respect of whom there is information on their participation in legalization (laundering) of criminal proceeds, and also to the Register of positions of national public officials.

14.2. For sending reports on suspicious operations (transactions) to the financial intelligence authority, the Company installs software for encryption of ARM FUS messages.

14.3. The Company shall submit to the financial intelligence authority the requested information or documents within the time limits established in the written request of the financial intelligence authority.

14.3.1. Within ten working days from the date of receipt of the request, the Company shall submit to the relevant supervisory authority the requested information or documents necessary for the performance of the functions of the supervisory authorities.

14.3.2. Information and documents, as well as the databases of the financial intelligence authority, are confidential and are protected in the established manner.

14.3.3. It shall not be deemed a violation or disclosure of official, company, tax, commercial, statistical secrecy and secrecy of communications (in terms of information on postal transfers of monetary funds): submission by the Company of information and documents upon request to the relevant supervisory authority.

15. APPLICATION OF TARGETED FINANCIAL SANCTIONS

15.1. The Company:

a) shall not, directly or indirectly (through third parties), in whole or in part, provide any funds or render financial services to individuals and legal

14.3.3. Не является нарушением или разглашением служебной, Компанией, налоговой, коммерческой, статистической тайны и тайны связи (в части информации о почтовых переводах денежных средств): Представление Компанией информации и документов по запросу, соответствующему проверяющему органу.

15. ПРИМЕНЕНИЕ ЦЕЛЕВЫХ ФИНАНСОВЫХ САНКЦИЙ

15.1. Компания:

- a) не должна прямо или косвенно (через третьих лиц), полностью или частично предоставлять любые средства или оказывать финансовые услуги физическим и юридическим лицам, группам, организациям, включенным в Санкционный перечень;
- b) обязаны безотлагательно заморозить операции (сделки) и (или) средства физического и юридического лица, группы, организации, включенных в Санкционный перечень, без предварительного уведомления данных лиц, на неопределенный срок.

При этом Компания в течение трех часов с момента выполнения требований пунктов а и б настоящей части сообщает об этом в орган финансовой разведки, в том числе о попытках совершения операций (сделок) физическими и юридическими лицами, группами, организациями, включенными в Санкционный перечень.

15.1.1. Замораживанию подлежат:

- a) любые средства, которыми владеют или которые контролируют лица, группы, организации, включенные в Санкционный перечень;
- b) средства, которыми полностью или на совместной основе, прямо или косвенно (через третьих лиц) владеют или которые контролируют лица, группы, организации, включенные в Санкционный перечень;
- c) средства, полученные или произведенные путем использования средств, которыми полностью или на совместной основе, прямо или косвенно (через третьих лиц) владеют или которые контролируют лица, группы, организации, включенные в Санкционный перечень;
- d) средства лиц, группы, организации, действующих по поручению или указанию лиц, групп, организаций, включенных в Санкционный перечень;
- e) средства, предназначенные для финансирования преступной и экстремистской деятельности, террористов и экстремистов, террористических и экстремистских

entities, groups, organizations included in the Sanctions List;

- b) shall immediately freeze operations (transactions) and/or funds of an individual and legal entity, group, organization included in the Sanctions List, without prior notice to such persons, for an indefinite period.

At the same time, the Company, within three hours from the moment of fulfilling the requirements of subparagraphs a and b of this paragraph, shall report this to the financial intelligence authority, including attempts to carry out operations (transactions) by individuals and legal entities, groups, organizations included in the Sanctions List.

15.1.1. The following shall be subject to freezing:

- a) any funds owned or controlled by persons, groups, organizations included in the Sanctions List;
- b) funds wholly or jointly, directly or indirectly (through third parties), owned or controlled by persons, groups, organizations included in the Sanctions List;
- c) funds received or produced through the use of funds wholly or jointly, directly or indirectly (through third parties), owned or controlled by persons, groups, organizations included in the Sanctions List;
- d) funds of persons, groups, organizations acting on behalf of or at the direction of persons, groups, organizations included in the Sanctions List;
- e) funds intended to finance criminal and extremist activity, terrorists and extremists, terrorist and extremist organizations, or persons proliferating weapons of mass destruction;
- f) funds determined in the relevant resolutions of the UN Security Council.

15.1.2. Operations (transactions) and/or funds of an individual and legal entity, group, organization included in the Sanctions List shall be frozen for an indefinite period and shall be unfrozen upon exclusion of the individual and legal entity, group, organization from the Sanctions List.

15.1.3. When applying targeted financial sanctions, protection of the rights of bona fide third parties acting in good faith shall be ensured in accordance with the legislation of the Kyrgyz Republic in the field of countering the financing of criminal activity and legalization (laundering) of criminal proceeds.

15.1.4. The procedure for freezing or unfreezing an operation (transaction) and/or funds, as well as the procedure for granting access to frozen funds and management of frozen funds, shall be established by the Cabinet of Ministers of the Kyrgyz Republic.

организаций либо лиц, распространяющих оружие массового уничтожения;

f) средства, определенные в соответствующих резолюциях Совета Безопасности ООН.

15.1.2. Операции (сделки) и (или) средства физического и юридического лица, группы, организации, включенных в Санкционный перечень, замораживаются на неопределенный срок и размораживаются при исключении физического и юридического лица, группы, организации из Санкционного перечня.

15.1.3. При применении целевых финансовых санкций обеспечивается защита прав добросовестных третьих лиц, действующих с честными намерениями, в соответствии с законодательством Кыргызской Республики в сфере противодействия финансированию преступной деятельности и легализации (отмыванию) преступных доходов.

15.1.4. Порядок замораживания или размораживания операции (сделки) и (или) средств, а также порядок предоставления доступа к замороженным средствам и управления замороженными средствами устанавливаются Кабинетом Министров Кыргызской Республики.

15.2. Меры по приостановлению операций (сделок).

15.2.1. Компания обязана незамедлительно приостановить операции (сделки), совершаемые физическим или юридическим лицом, группой, организацией, включенными в Перечень лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов, и сообщить об этом в орган финансовой разведки в течение трех часов с момента приостановления операции (сделки).

15.2.2. Операции (сделки) приостанавливаются до принятия решения о наложении ареста на имущество, принятого в соответствии с уголовно-процессуальным законодательством Кыргызской Республики. В случае непринятия решения о наложении ареста на имущество приостановленная операция (сделка) проводится в установленном порядке.

15.2.3. Порядок формирования Перечня лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов, и порядок исключения из него, а также порядок его опубликования устанавливаются Кабинетом Министров Кыргызской Республики.

15.2. Measures for suspension of operations (transactions).

15.2.1. The Company shall immediately suspend operations (transactions) carried out by an individual or legal entity, group, organization included in the List of persons, groups, organizations in respect of whom there is information on their participation in legalization (laundering) of criminal proceeds, and shall report this to the financial intelligence authority within three hours from the moment of suspension of the operation (transaction).

15.2.2. Operations (transactions) shall be suspended until a decision is made to seize property, adopted in accordance with the criminal procedure legislation of the Kyrgyz Republic. In the event no decision is made to seize property, the suspended operation (transaction) shall be carried out in the established manner.

15.2.3. The procedure for formation of the List of persons, groups, organizations in respect of whom there is information on their participation in legalization (laundering) of criminal proceeds, and the procedure for exclusion therefrom, as well as the procedure for its publication, shall be established by the Cabinet of Ministers of the Kyrgyz Republic.

16. PROCEDURE FOR ORGANIZING IN THE COMPANY A SYSTEM FOR THE IMPLEMENTATION OF THE INTERNAL CONTROL PROGRAM

16.1. The function of control over the implementation of internal control for CFCA/LCP in the Company is assigned to the highest management body - the Participant of the Company.

16.1.1. The Participant of the Company is responsible for:

a) ensuring adequate and effective activity of the Company in the field of CFCA/LCP, as well as preventing the involvement of the Company in

16. ПРОЦЕДУРА ПО ОРГАНИЗАЦИИ В КОМПАНИИ СИСТЕМЫ ДЛЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ВНУТРЕННЕГО КОНТРОЛЯ

16.1. Функция контроля над осуществлением внутреннего контроля по ПФПД ЛПД в Компании возлагается на высший орган управления - Участника Компании.

16.1.1. Участник Компании несет ответственность за:

- a) за обеспечение адекватной и эффективной деятельностью Компании в сфере ПФПД ЛПД, а также предотвращения вовлечения Компании в проведение операций, имеющих признаки подозрительных операций;
- b) утверждение адекватной и эффективной политики в сфере ПФПД ЛПД;
- c) утверждение программы внутреннего контроля в сфере ПФПД ЛПД, а также осуществление контроля за их реализацией;
- d) определение мер по обеспечению эффективной работы должностного лица по ПФПД ЛПД;
- e) назначение на должность и освобождение от должности должностного лица по ПФПД ЛПД;
- f) рассмотрение отчета службы внутреннего аудита и отчетов должностного лица по ПФПД ЛПД;
- g) определение мер, направленных на устранение недостатков в сфере ПФПД ЛПД, выявленных службой внутреннего аудита и указанных в отчете должностного лица по ПФПД ЛПД, а также контролирует их реализацию;
- h) Участник Компании должен предпринимать исчерпывающие меры в целях недопущения вовлечения Компании в проведение операций, имеющих признаки подозрительных операций.

16.1.2. Комплаенс офицер Компании несет ответственность за:

- a) обеспечение внедрения политики и программы внутреннего контроля в сфере ПФПД ЛПД, утвержденных Участником Компании;
- b) обеспечение и контроль исполнения законодательства КР в сфере ПФПД ЛПД;
- c) обеспечение обучения сотрудников Компании в области ПФПД ЛПД;
- d) обеспечение реализации мер, направленных на устранение недостатков, имеющихся во внутренних мерах, процедурах и системе внутреннего контроля, а также обеспечение проведения независимого аудита;
- e) обеспечение исполнения требований нормативных правовых актов КР, касающихся

carrying out operations having signs of suspicious operations;

b) approval of an adequate and effective policy in the field of CFCA/LCP;

c) approval of the internal control program in the field of CFCA/LCP, as well as exercising control over its implementation;

d) determination of measures to ensure the effective work of the official for CFCA/LCP;

e) appointment to the position and dismissal from the position of the official for CFCA/LCP;

f) consideration of the report of the internal audit service and reports of the official for CFCA/LCP;

g) determination of measures aimed at eliminating deficiencies in the field of CFCA/LCP identified by the internal audit service and indicated in the report of the official for CFCA/LCP, and also control over their implementation;

h) the Participant of the Company shall take exhaustive measures for the purpose of preventing the involvement of the Company in carrying out operations having signs of suspicious operations.

16.1.2. The Company's Compliance Officer is responsible for:

a) ensuring the implementation of the policy and internal control program in the field of CFCA/LCP approved by the Participant of the Company;

b) ensuring and controlling compliance with the legislation of the Kyrgyz Republic in the field of CFCA/LCP;

c) ensuring the training of the Company's employees in the field of CFCA/LCP;

d) ensuring the implementation of measures aimed at eliminating deficiencies existing in internal measures, procedures and the internal control system, as well as ensuring the conduct of an independent audit;

e) ensuring compliance with the requirements of the regulatory legal acts of the Kyrgyz Republic concerning the opening of Accounts, accounts (including identification and verification of clients and the beneficial owner), carrying out operations on accounts, and termination of agreements with clients (account holders).

17. PROCEDURE FOR APPROVAL OF KEY OFFICIALS OF THE VA EXCHANGE OPERATOR

17.1. The virtual asset exchange operator shall be obliged to obtain approval from the authorized body for its officials, who must not be included in sanctions lists.

открытия Учетных записей, счетов (в том числе идентификации и верификации клиентов и бенефициарного владельца), проведения операций по счетам и расторжения договоров с клиентами (владельцами счетов).

17. ПРОЦЕДУРА СОГЛАСОВАНИЯ КЛЮЧЕВЫХ ДОЛЖНОСТНЫХ ЛИЦ ОПЕРАТОРА ОБМЕНА ВА

17.1. Оператор обмена виртуальных активов обязан согласовывать своих должностных лиц, которые должны отсутствовать в санкционных списках, с уполномоченным органом

17.2. Должностными лицами оператора обмена виртуальных активов, кандидатуры которых подлежат согласованию, являются:

руководитель и члены совета директоров (при наличии);

руководитель (лицо, единолично осуществляющее функции исполнительного органа) и члены исполнительного органа;

главный бухгалтер или единственный бухгалтер;

уполномоченный сотрудник или директор по рискам и комплаенсу.

17.3. Должностное лицо оператора обмена виртуальных активов вправе занимать свою должность без согласования не более 45 календарных дней со дня его назначения (избрания).

17.4. По истечении срока 45 дней, и в случаях непредставления полного пакета документов на согласование либо отказа в согласовании оператор обмена виртуальных активов обязан расторгнуть трудовой договор с данным лицом, либо в случае отсутствия трудового договора принять меры по прекращению полномочий данного должностного лица.

17.5. Запрещается исполнение обязанностей (замещение временно отсутствующего) должностного лица оператора обмена виртуальных активов без согласования свыше, установленного срока 45 дней.

17.6. Для согласования должностного лица оператор обмена виртуальных активов представляет в уполномоченный орган письмо о согласовании (отдельно) каждой кандидатуры с приложением заверенных копий следующих документов:

- решение об избрании/назначении кандидатуры;

- удостоверение личности кандидата;

- оригинал справки об отсутствии судимости;

- оригинал анкеты кандидата по установленной форме

17.7. При изменении в составе должностных лиц, прошедших процедуру согласования,

17.2. The officials of the virtual asset exchange operator whose candidacies are subject to approval are:

the head and members of the board of directors (if any);

t

the head (the person solely performing the functions of the executive body) and members of the executive body;

the chief accountant or sole accountant;

the authorized employee or the director for risks and compliance.

17.3. An official of the virtual asset exchange operator shall have the right to hold his position without approval for no more than 45 calendar days from the date of his appointment (election).

17.4. Upon expiration of the 45-day period, and in cases of failure to submit a complete package of documents for approval or refusal of approval, the virtual asset exchange operator shall be obliged to terminate the employment contract with such person, or, in the absence of an employment contract, take measures to terminate the powers of such official.

17.5. It is prohibited to perform the duties of an official of the virtual asset exchange operator (to substitute for a temporarily absent official) without approval for more than the established period of 45 days.

17.6. For the approval of an official, the virtual asset exchange operator shall submit to the authorized body a letter for approval of each candidacy (separately), with attached certified copies of the following documents:

- decision on the election/appointment of the candidate;

- candidate's identity document;

- original certificate of no criminal record;

- original candidate's questionnaire in the prescribed form.

17.7. In the event of changes in the composition of officials who have undergone the approval procedure, the virtual asset exchange operator shall, within 5 (five) working days from the date of election (appointment) of the new official, be obliged to submit to the authorized body a notice of changes. A letter for approval of the new candidacy shall be submitted to the authorized body within 10 (ten) working days from the date of election (appointment), with the documents listed above attached.

17.8. In the event of changes in the information contained in the items of the questionnaire, officials who have undergone approval shall be obliged to notify the authorized body thereof (in writing) within 10 (ten) working days after the changes.

оператор обмена виртуальных активов в течение 5 (пять) рабочих дней со дня избрания (назначения) нового должностного лица обязан предоставить в уполномоченный орган уведомление об изменениях. Письмо о согласовании новой кандидатуры представляется в уполномоченный орган в течение 10 (десять) рабочих дней со дня избрания (назначения) с приложением перечисленных выше документов.

17.8. При изменении информации, содержащейся в пунктах анкеты, должностные лица, прошедшие согласование, обязаны уведомлять об этом (в письменной форме) уполномоченный орган в течение 10 (десять) рабочих дней после изменений.

17.9. Документы на согласование должностного лица представляются на государственном или официальном языках.

18. ПОРЯДОК ПРОВЕДЕНИЯ ОБУЧЕНИЯ СОТРУДНИКО КОМПАНИИ ПО ПФПД ЛПД

18.1. Компания разрабатывает процедуру базового обучения кадров по вопросам ПФПД ЛПД.

18.1.1. Базовое обучение проводится в соответствии с планом обучения, Компании, в соответствии с законодательством Кыргызской Республики в сфере ПФПД ЛПД.

Базовое обучение сотрудников Компании осуществляется в следующих формах:

- a) вводное (первичное) обучение;
- b) внеплановое (целевое) обучение;
- c) плановое обучение.

18.1.2. Вводное (первичное) обучение проводится в целях ознакомления с законодательством Кыргызской Республики в сфере ПФПД ЛПД и внутренними документами Компании по ПФПД ЛПД.

18.1.3. Вводное (первичное) обучение проводится при приеме или переводе на работу в службу по комплаенс контролю. По истечении трех месяцев с даты приема или перевода сотрудника проводится оценка уровня его знаний в сфере ПФПД ЛПД.

18.1.4. Внеплановое (целевое) обучение по ПФПД ЛПД проводится в следующих случаях:

- при изменении действующих или вступлении в силу новых нормативных правовых актов Кыргызской Республики в сфере ПФПД ЛПД;
- при введении новых или изменении действующих программ по комплаенс контролю по ПФПД ЛПД;

17.9. Documents for approval of an official shall be submitted in the state or official language

18. PROCEDURE FOR CONDUCTING TRAINING OF COMPANY EMPLOYEES ON CFCA/LCP

18.1. The Company develops a procedure for basic training of personnel on issues of CFCA/LCP.

18.1.1. Basic training is conducted in accordance with the Company's training plan, in accordance with the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

Basic training of the Company's employees is carried out in the following forms:

- a) introductory (initial) training;
- b) unscheduled (targeted) training;
- c) scheduled training.

18.1.2. Introductory (initial) training is conducted for the purpose of familiarization with the legislation of the Kyrgyz Republic in the field of CFCA/LCP and the Company's internal documents on CFCA/LCP.

18.1.3. Introductory (initial) training is conducted upon hiring or transfer to work in the compliance control service. Upon expiration of three months from the date of hiring or transfer of the employee, an assessment of the level of his knowledge in the field of CFCA/LCP is conducted.

18.1.4. Unscheduled (targeted) training on CFCA/LCP is conducted in the following cases:

- upon amendment of existing or entry into force of new regulatory legal acts of the Kyrgyz Republic in the field of CFCA/LCP;
- upon introduction of new or amendment of existing compliance control programs on CFCA/LCP;
- upon transfer of an employee to another permanent job within the Company's divisions, in a case where the knowledge he has in the field of CFCA/LCP is insufficient for performance of his functions;
- upon assigning to an employee work in the field of CFCA/LCP not stipulated by the labor contract concluded with him, where this does not entail a change in the terms of such contract.

18.1.5. Scheduled training of the Company's employees is carried out regularly, but not less than once a year.

- при переводе сотрудника на другую постоянную работу в рамках подразделений Компании, в случае, когда имеющихся у него знаний в области ПФПД ЛПД недостаточно для выполнения своих функций;

- при поручении сотруднику работы в области ПФПД ЛПД, не обусловленной заключенным с ним трудовым договором, когда это не влечет за собой изменения условий данного договора.

18.1.5. Плановое обучение сотрудников Компании осуществляется регулярно, но не реже одного раза в год.

18.1.6. Плановое обучение в сфере ПФПД ЛПД проводится путем участия сотрудников в конференциях, семинарах и иных обучающих мероприятиях, проводимых образовательными организациями согласно программам обучения образовательных организаций.

18.1.7. Проверка знаний сотрудников в сфере ПФПД ЛПД проводится не реже одного раза в год в соответствии с планом обучения Компании.

18.1.8. При выявлении недостаточного уровня знаний сотрудника в сфере ПФПД ЛПД, его руководитель принимает решение о целесообразности его дальнейшего использования исключительно на участках работы, не связанных с выполнением требований ПФПД ЛПД, или направлении его на обучение для повышения квалификации и профессиональной переподготовки.

18.1.9. Повышение квалификации и профессиональная переподготовка кадров. Целью повышения квалификации и профессиональной переподготовки кадров является получение работниками дополнительных профессиональных знаний в сфере ПФПД ЛПД, необходимых для соблюдения законодательства Кыргызской Республики в сфере ПФПД ЛПД.

18.1.10. Компания ежегодно разрабатывает график повышения квалификации и профессиональной переподготовки своих кадров в сфере ПФПД ЛПД, с учетом требований законодательства Кыргызской Республики в сфере ПФПД ЛПД, а также особенностей своей деятельности, а также не позднее 15 декабря текущего года направляют данный график в Учебно-методический центр Государственной службы финансовой разведки при Министерстве финансов Кыргызской Республики для оценки потребностей в обучении.

18.1.11. Компания должна регулярно, но не реже одного раза в год (в соответствии с графиком), направлять сотрудников службы

18.1.6. Scheduled training in the field of CFCA/LCP is conducted by participation of employees in conferences, seminars and other training events conducted by educational organizations in accordance with the training programs of educational organizations.

18.1.7. Testing of employees' knowledge in the field of CFCA/LCP is conducted not less than once a year in accordance with the Company's training plan.

18.1.8. Upon identification of an insufficient level of an employee's knowledge in the field of CFCA/LCP, his manager makes a decision on the expediency of his further use exclusively in work areas not connected with fulfillment of the requirements of CFCA/LCP, or on sending him for training for advanced qualification and professional retraining.

18.1.9. Advanced qualification and professional retraining of personnel. The purpose of advanced qualification and professional retraining of personnel is the receipt by employees of additional professional knowledge in the field of CFCA/LCP necessary for compliance with the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

18.1.10. The Company annually develops a schedule for advanced qualification and professional retraining of its personnel in the field of CFCA/LCP, taking into account the requirements of the legislation of the Kyrgyz Republic in the field of CFCA/LCP, as well as the specifics of its activity, and also no later than December 15 of the current year sends this schedule to the Training and Methodological Center of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic for assessment of training needs.

18.1.11. The Company shall regularly, but not less than once a year (in accordance with the schedule), send employees of the internal control service and other employees directly working with clients, including the Company's managers, to an educational organization for undergoing advanced qualification and professional retraining courses (hereinafter – training). The Company shall send the list of personnel who have undergone training in the field of CFCA/LCP, in written and electronic form, to the financial intelligence authority of the Kyrgyz Republic no later than December 25 of the current year for the purposes of centralized accounting of trained personnel and formation of the relevant database.

18.1.12. The same manager or employee of the Company is not sent annually for undergoing training.

Training of personnel is conducted in the following cases:

внутреннего контроля и других сотрудников, непосредственно работающих с клиентами, в том числе руководителей Компании, в образовательную организацию для прохождения курсов повышения квалификации и профессиональной переподготовки (далее – обучение). Компания должна направить список кадров, прошедших обучение в сфере ПФПД ЛПД, в письменном и электронном виде в орган финансовой разведки Кыргызской Республики не позднее 25 декабря текущего года в целях централизованного учета подготовленных кадров и формирования соответствующей базы данных.

18.1.12. Один и тот же руководитель или сотрудник Компании ежегодно не направляется для прохождения обучения.

Обучение кадров проводится в следующих случаях:

- при приеме на работу;
- при переводе работника на другую постоянную работу (временную работу) в рамках подразделений, в случае, когда имеющихся у него знаний в сфере ПФПД ЛПД недостаточно для соблюдения законодательства Кыргызской Республики в сфере ПФПД ЛПД;
- при принятии новых нормативных правовых актов Кыргызской Республики в сфере ПФПД ЛПД;
- при нарушении работниками требований системы внутреннего контроля по ПФПД ЛПД;
- по решению руководства Компании.

Ответственность за организацию и своевременность обучения кадров несет руководитель Компании.

19. ПОРЯДОК ПРОВЕДЕНИЯ НЕЗАВИСИМОГО АУДИТА

19.1. Компания должна проводить на постоянной основе, но не менее одного раза в год независимый аудит, который включает следующее:

- 1) оценка эффективности внутренних мер, процедур и системы контроля финансового учреждения и нефинансовой категории лиц по вопросам ПФПД ЛПД;
- 2) оценка применяемых мер по оценке рисков;
- 3) оценка используемого программного обеспечения по выявлению и формированию сообщений об операциях (сделках), подлежащих контролю и сообщению;
- 4) выборочное тестирование деятельности службы внутреннего контроля, включая применяемое программное обеспечение;

- upon hiring;
- upon transfer of an employee to another permanent job (temporary job) within divisions, in a case where the knowledge he has in the field of CFCA/LCP is insufficient for compliance with the legislation of the Kyrgyz Republic in the field of CFCA/LCP;
- upon adoption of new regulatory legal acts of the Kyrgyz Republic in the field of CFCA/LCP;
- upon violation by employees of the requirements of the internal control system on CFCA/LCP;
- by decision of the Company's management.

Responsibility for the organization and timeliness of training of personnel is borne by the head of the Company.

19. PROCEDURE FOR CONDUCTING AN INDEPENDENT AUDIT

19.1. The Company must conduct, on a permanent basis, but not less than once a year, an independent audit, which includes the following:

- 1) assessment of the effectiveness of internal measures, procedures and the control system of the financial institution and non-financial category of persons on issues of CFCA/LCP;
- 2) assessment of the applied risk assessment measures;
- 3) assessment of the software used to identify and generate reports on operations (transactions) subject to control and reporting;
- 4) selective testing of the activities of the internal control service, including the software used;
- 5) verification of compliance of the reports of the internal control service and training programs of employees of the financial institution and non-financial category of persons;
- 6) assessment of the measures applied by the management of the financial institution and non-financial category of persons to eliminate violations of the legislation of the Kyrgyz Republic in the field of CFCA/LCP.

19.2. An independent audit is conducted by internal auditors or by a person/division responsible for the audit of the Company, and in their absence - by

5) проверка соответствия отчетов службы внутреннего контроля и программ обучения сотрудников финансового учреждения и нефинансовой категории лиц;

6) оценка мер, применяемых руководством финансового учреждения и нефинансовой категории лиц, по устранению нарушений законодательства Кыргызской Республики в сфере ПФПД ЛПД.

19.2. Независимый аудит проводится внутренними аудиторами или лицом/подразделением, ответственным за аудит Компании, а в случае их отсутствия - внешними аудиторами (индивидуальный аудитор) и (или) аудиторскими организациями, зарегистрированными в соответствии с законодательством Кыргызской Республики об аудиторской деятельности.

19.3. В целях проведения качественного и всестороннего независимого аудита аудитор проводит консультации со службой внутреннего контроля для получения информации о внутренних мерах, процедурах и системах контроля в сфере ПФПД ЛПД, а также имеющихся проблемах. Аудитор должен иметь доступ ко всем материалам и отчетам финансового учреждения и нефинансовой категории лиц.

20. ПОРЯДОК ОРГАНИЗАЦИИ КОМПАНИЕЙ РАБОТЫ ПО ОТКАЗУ ОТ ПРИНЯТИЯ НА ОБСЛУЖИВАНИЕ/ЗАКЛЮЧЕНИЯ ДОГОВОРА УСЛУГ И ПО ОТКАЗУ ВЫПОЛНЕНИЯ КОМПАНИЕЙ РАСПОРЯЖЕНИЙ/ЗАЯВОК КЛИЕНТА ОБ ОСУЩЕСТВЛЕНИИ ОПЕРАЦИЙ (СДЕЛОК)

20.1. Компания должна отказать клиенту в открытии счета (заключении договора) или проведении операций по счету, если:

- не представлены соответствующие документы, необходимые для выполнения требований по открытию счета/ учетной записи (заключении договора) и проведению операций по нему, идентификации и верификации клиента и бенефициарного владельца и проведения других мер надлежащей проверки клиента;

- представлены явно недостоверные документы.

При этом Компания должна в установленном порядке направить соответствующее сообщение в орган финансовой разведки в течение одного рабочего дня со дня принятия решения об отказе в обслуживании клиента.

external auditors (individual auditor) and/or audit organizations registered in accordance with the legislation of the Kyrgyz Republic on auditing activity.

19.3. For the purpose of conducting a high-quality and comprehensive independent audit, the auditor conducts consultations with the internal control service to obtain information on internal measures, procedures and control systems in the field of CFCA/LCP, as well as existing problems. The auditor must have access to all materials and reports of the financial institution and non-financial category of persons.

20. PROCEDURE FOR ORGANIZING THE COMPANY'S WORK ON REFUSAL TO ACCEPT FOR SERVICING / CONCLUSION OF A SERVICE AGREEMENT AND ON REFUSAL BY THE COMPANY TO EXECUTE THE CLIENT'S ORDERS / APPLICATIONS FOR CARRYING OUT OPERATIONS (TRANSACTIONS)

20.1. The Company must refuse the client to open an account (conclude an agreement) or carry out operations on the account if:

- the relevant documents necessary to fulfill the requirements for opening an account/account record (concluding an agreement) and carrying out operations thereunder, identification and verification of the client and beneficial owner, and carrying out other customer due diligence measures have not been submitted;

- clearly unreliable documents have been submitted.

At the same time, the Company must, in the established manner, send the relevant report to the financial intelligence authority within one working day from the date of making the decision to refuse servicing the client. Also, within one working day from the date of making one of the following decisions:

- on suspension or termination of the established business relationship with the client (refusal of servicing) and termination of the agreement concluded with the client;

- on refusal to carry out an operation (transaction).

20.2. In the event that, when opening an account (concluding an agreement) or carrying out operations on the account, the Company has suspicions that the operations (transactions) are connected with the financing of criminal activity

Также, в течение одного рабочего дня со дня принятия одного из следующих решений:

- о приостановлении или прекращении установленного делового отношения с клиентом (отказ в обслуживании) и расторжении заключенного договора с клиентом;
- об отказе в осуществлении операции (сделки).

20.2. В случае если при открытии счета (заключении договора) или проведении операций по счету у Компании возникнут подозрения, что операции (сделки) связаны с финансированием преступной деятельности и легализацией (отмыванием) преступных доходов, Компания должна применить следующие меры:

- провести идентификацию и верификацию клиента и бенефициарного владельца, независимо от любых исключений или установленных пороговых значений;
- направить сообщение о подозрительной операции (сделке) в орган финансовой разведки в течение 5 (пяти) часов с момента признания операции (сделки) подозрительной.

20.3. В случае если Компания убеждена в том, что проведение надлежащей проверки клиента приведет к разглашению информации о возникших подозрениях, Компания не принимает меры по надлежащей проверке клиента и направляет сообщение о подозрительной операции (сделке) в орган финансовой разведки.

20.4. Если в отношении клиента или бенефициарного владельца имеются сведения об участии в преступной или экстремистской деятельности и распространении оружия массового уничтожения, полученные в соответствии с нормами законодательства Кыргызской Республики, Компания должна без предварительного уведомления клиента безотлагательно заморозить операцию (сделку) и/или средства клиента на неопределенный срок, включенного в Санкционный перечень, и в течение 3 (трех) часов с момента замораживания направить сообщение в орган финансовой разведки.

21. ПОРЯДОК ОПУБЛИКОВАНИЯ ПЕРЕЧНЯ ЛИЦ, ГРУПП, ОРГАНИЗАЦИЙ, В ОТНОШЕНИИ КОТОРЫХ ИМЕЮТСЯ СВЕДЕНИЯ ОБ ИХ УЧАСТИИ В ЛЕГАЛИЗАЦИИ (ОТМЫВАНИИ) ПРЕСТУПНЫХ ДОХОДОВ

21.1. Сводный санкционный перечень Кыргызской Республики публикуется и

and legalization (laundering) of criminal proceeds, the Company must apply the following measures:

- conduct identification and verification of the client and beneficial owner, regardless of any exceptions or established threshold values;
 - send a report on a suspicious operation (transaction) to the financial intelligence authority within 5 (five) hours from the moment the operation (transaction) is recognized as suspicious.
- 20.3. In the event that the Company is convinced that conducting customer due diligence will lead to disclosure of information on the suspicions that have arisen, the Company does not take customer due diligence measures and sends a report on a suspicious operation (transaction) to the financial intelligence authority.

20.4. If there is information regarding the client or beneficial owner about participation in criminal or extremist activity and proliferation of weapons of mass destruction, obtained in accordance with the norms of the legislation of the Kyrgyz Republic, the Company must, without prior notification of the client, immediately freeze the operation (transaction) and/or the client's funds for an indefinite period, included in the Sanctions List, and within 3 (three) hours from the moment of freezing send a report to the financial intelligence authority.

21. PROCEDURE FOR PUBLICATION OF THE LIST OF PERSONS, GROUPS, ORGANIZATIONS IN RESPECT OF WHICH THERE IS INFORMATION ABOUT THEIR PARTICIPATION IN LEGALIZATION (LAUNDERING) OF CRIMINAL PROCEEDS

21.1. The Consolidated Sanctions List of the Kyrgyz Republic is published and posted on the official website of the financial intelligence authority, in the "Lists" section. The Consolidated Sanctions List of the Kyrgyz Republic is posted in the form of an electronic database determined by the financial intelligence authority. The structure and format of the Consolidated Sanctions List of the Kyrgyz Republic are determined by the financial intelligence authority.

21.1.1. The updated version of the Consolidated Sanctions List of the Kyrgyz Republic and the

размещается на официальном сайте органа финансовой разведки, в разделе «Перечни». Сводный санкционный перечень Кыргызской Республики размещается в виде электронной базы данных, определяемой органом финансовой разведки. Структура и формат Сводного санкционного перечня Кыргызской Республики определяются органом финансовой разведки.

21.1.1. Обновленная редакция Сводного санкционного перечня Кыргызской Республики и приказ органа финансовой разведки о внесении изменений или дополнений в Сводный санкционный перечень Кыргызской Республики публикуются на официальном сайте органа финансовой разведки в течение одного часа с момента подписания данного приказа.

21.1.2. Публикация Сводного санкционного перечня Кыргызской Республики на официальном сайте органа финансовой разведки считается официальным опубликованием.

21.1.3. В течение трех часов с момента опубликования на официальном сайте органа финансовой разведки информации об опубликовании новой редакции Сводного санкционного перечня Кыргызской Республики, финансовым учреждениям и нефинансовым категориям лиц направляется соответствующая информация по электронным каналам связи, определенным органом финансовой разведки.

21.1.4. Уполномоченное лицо по ПФПД ЛПД регулярно следит за обновлениями на официальном сайте и приводит в соответствие данные.

22. ОТВЕТСТВЕННОСТЬ ЗА НЕСОБЛЮДЕНИЕ ПФПД ЛПД

22.1. Нарушение требований, предусмотренных Законом КР «О ПФПД ЛПД», влечет административную ответственность в порядке, предусмотренном законодательством КР.

22.2. Руководство и сотрудники Компании, в том числе бывшие, которые в соответствии с Законом КР «О ПФПД ЛПД» имеют или имели доступ к информации, получаемой от Компании, несут уголовную ответственность за незаконное разглашение, использование Компанией, коммерческой или иной тайны, злоупотребление служебным положением в соответствии с уголовным законодательством КР.

22.3. Сотрудники Компании, в том числе бывшие, несут ответственность за разглашение

order of the financial intelligence authority on making amendments or additions to the Consolidated Sanctions List of the Kyrgyz Republic are published on the official website of the financial intelligence authority within one hour from the moment of signing this order.

21.1.2. Publication of the Consolidated Sanctions List of the Kyrgyz Republic on the official website of the financial intelligence authority is considered official publication.

21.1.3. Within three hours from the moment of publication on the official website of the financial intelligence authority of information on publication of a new version of the Consolidated Sanctions List of the Kyrgyz Republic, the relevant information is sent to financial institutions and non-financial categories of persons via electronic communication channels determined by the financial intelligence authority.

21.1.4. The authorized person for CFCA/LCP regularly monitors updates on the official website and brings the data into conformity.

22. LIABILITY FOR NON-COMPLIANCE WITH CFCA/LCP

22.1. Violation of the requirements provided for by the Law of the Kyrgyz Republic “On CFCA/LCP” entails administrative liability in the manner provided for by the legislation of the Kyrgyz Republic.

22.2. The management and employees of the Company, including former ones, who in accordance with the Law of the Kyrgyz Republic “On CFTD/LCP” have or had access to information received from the Company, bear criminal liability for unlawful disclosure, use by the Company, of commercial or other secret, abuse of official position in accordance with the criminal legislation of the Kyrgyz Republic.

22.3. Employees of the Company, including former ones, bear responsibility for disclosure of the fact of execution of requests and sending information to the SFRS in accordance with the legislation of the Kyrgyz Republic.

23. FINAL PROVISIONS

23.1. Every employee of the Company who participates in the implementation of this Program is obliged to study it and be guided by it in the performance of his duties.

факта исполнения запросов и направления информации в ГСФР в соответствии с законодательством Кыргызской Республики.

23. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

23.1. Каждый сотрудник Компании, который участвует в реализации настоящей Программы, обязан изучить ее и руководствоваться при выполнении своих обязанностей.

23.2. Основными задачами сотрудников Компании в области противодействия финансированию преступной деятельности и легализации преступных доходов, являются:

- Участие в процессе идентификации клиентов, изучения их деятельности и мониторинга сделок;
- Участие в процессе мониторинга сделок клиентов выявлять операции, которые считаются необычными или подозрительными финансовыми сделками;
- Исключение возможности вовлечения Компании и участия его служащих в осуществлении финансирования преступной деятельности и легализации (отмывания) преступных доходов;
- Обеспечение надежности и безопасности в сфере ПФПД ЛПД;
- Защита деловой репутации и торговой марки Компании.

23.3. Настоящая Программа вступает в силу с момента утверждения.

23.2. The main tasks of the Company's employees in the field of countering the financing of criminal activity and legalization of criminal proceeds are:

- Participation in the process of client identification, study of their activities and transaction monitoring;
- Participation in the process of monitoring client transactions to identify operations that are considered unusual or suspicious financial transactions;
- Exclusion of the possibility of involvement of the Company and participation of its employees in financing criminal activity and legalization (laundering) of criminal proceeds;
- Ensuring reliability and security in the field of CFCA/LCP;
- Protection of the business reputation and trademark of the Company.

23.3. This Program enters into force from the moment of approval.

Amendments and additions to this Program shall be approved by the Participant of the Company.

Изменения и дополнения в настоящую Программу утверждаются Участником Компании.

Директор / Director

_____/Лотоев Борис / Lotoev Boris/